The Effects of Cyber Supply Chain Attacks and Mitigation Strategies

Ravi Das

CRC Press
Taylor & Francis Group

The Effects of Cyber Supply Chain Attacks and Mitigation Strategies

Ravi Das

CRC Press
Taylor & Francis Group

The Effects of Cyber Supply Chain Attacks and Mitigation Strategies

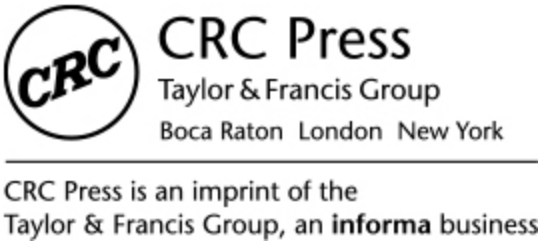
The world of Cybersecurity today is becoming increasingly complex. There are many new Threat Variants that are coming out, but many of them are just tweaked versions of some of the oldest ones, such as Phishing and Social Engineering. In today's world, Threat Variants are becoming much complex, stealthier, and covert. Thus, it makes it almost impossible to detect them on time before the actual damage is done.

One such example of this are what is known as Supply Chain Attacks. What makes this different from the other Threat Variants is that through just one point of entry, the Cyberattacker can deploy a Malicious Payload and impact thousands of victims. This is what this book is about, and it covers the following:

- Important Cybersecurity Concepts
- A introduction to Supply Chain Attacks and its impact on the Critical Infrastructure in the United States.
- Examples of Supply Chain Attacks, most notably those of Solar Winds and Crowd Strike.
- Mitigation strategies that the CISO and their IT Security team can take to thwart off Supply Chain Attacks.

The Effects of Cyber Supply Chain Attacks and Mitigation Strategies

Ravi Das



Designed cover image: Shutterstock Image ID 2176617569
First edition published 2026
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431
and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN
CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 978-1-032-95531-5 (hbk)
ISBN: 978-1-032-95643-5 (pbk)
ISBN: 978-1-003-58591-6 (ebk)
DOI: 10.1201/9781003585916
Typeset in Sabon
by SPi Technologies India Pvt Ltd (Straive)

This book is dedicated to my Lord and Savior, Jesus Christ, the Grand Designer of the Universe, and to my parents, Dr. Gopal Das and Mrs. Kunda Das.
My loving cats, Fifi and Bubu, and guinea pig, Noodles.

This book is also dedicated to:

Richard and Gwynda Bowman
Jaya Chandra
Tim Auckley
Patricia Bornhofen
Ashish Das
Caylee Gibbons
Rory Maxfield
Caylee Gibbons
Lynette Lambing

Contents

Acknowledgments

I would like to thank Ms. Gabrielle Williams, my editor, who made this book into a reality.

Author biography

Ravi Das is a technical writer in the Cybersecurity realm. He also does Cybersecurity consulting on the side through his private practice, M L Tech, Inc. He also holds the Certification in Cybersecurity from the ISC(2).

Chapter 1
An overview into Cybersecurity

DOI: 10.1201/9781003585916-1

When one thinks of security, very often the image of guards comes to mind. While this is true to a certain extent, this term has now reached and pushed the envelope of its context and scope. For example, just within the last ten years or so, Cybersecurity has now taken the major foothold in terms of attention not only by the media but even in terms of actual impacts to victims as well. These can range from anything, from being impacted by a Phishing email to becoming prey to a Ransomware Attack, where the victim is very often tricked into making a payment in order to unlock their device and reclaim their heisted files, or worst yet, even becoming the victim of an Extortion Attack.

But, as noted, there are other extremes as well. For example, the victim could become paralyzed by a case of Identity Theft, where it can take many years just to reclaim their identity once it has been stolen. Or the victim could fall prey to a Social Engineering attack, in which the Cyberattacker builds a convincing rapport over a period of time, only to con the victim to doing something very wrong, such as wiring a large sum of money to a phony offshore account.

Cyberbullying

But probably one of the worst forms of a Cyberattack comes in the form of Bulling, especially as it relates to Cyberbullying. The latter can be technically defined as follows:

> Cyberbullying is the use of technology to harass, threaten, embarrass, or target another person. Online threats and mean, aggressive, or rude texts, tweets, posts, or messages all count. So does posting personal information, pictures, or videos designed to hurt or embarrass someone else.
>
> Cyberbullying also includes photos, messages, or pages that don't get taken down, even after the person has been asked to do so. In other words, it's anything that gets posted online and is meant to hurt, harass, or upset someone else.
>
> (Cyberbullying (for Teens) | Nemours KidsHealth)

So, as one can see from the above definition, Cyberbullying actually can be considered a "step up" from the normal forms of just Bullying. For example, rather than having physical interaction, it all takes place in the realm of the Internet. One of the most popular places for this to occur is on all of the Social Media Platforms, which include the likes of Facebook, X (formerly known as "Twitter"), LinkedIn, Instagram, Pinterest, etc. But it is also very important to keep in mind that the perpetrator who is instigating the Cyberbullying Attack can literally be thousands of miles away, in a totally different country.

Thus, if the perpetrator were ever to be identified, there would be very little that can be done in order to bring him or her to justice, as they would be bound by the laws of their own country. In other words, even the thoughts of legal extradition would be extremely far fetched, but also the impacts to the victim of a Cyberbullying Attack can be detrimental. For

example, not only can they suffer from long mental illness as a result of it, but the victim, if the Cyberbullying goes on long enough, can even become suicidal.

- Or worst yet, the perpetrator, over a longer period of time, can gain complete control over their victim and literally "brainwash" them to do things that they have never done before. In other words, this can be viewed as an ultra-sophisticated form of a Social Engineering attack. In fact, one of our previously published books was devoted exclusively to Cyberbullying. It is titled "Generative AI and Cyberbullying". It can be seen at the link below:

  Generative AI and Cyberbullying – 1st Edition – Ravindra Das – Routledge

The dawn of generative AI

Although the threat variants we have just touched on can be very dangerous to the victim, there is now a new trend that is occurring which can make the threat variants even deadlier. This has been brought on by the evolution of Generative AI. It can be technically defined as follows:

> Generative AI refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.
>
> (What is generative AI? – IBM Research)

Generative AI is actually a subset of all of these major components of artificial intelligence (AI):

- Machine Learning

- Neural Networks
- Large Language Models (LLMs)
- Natural Language Procession

With the traditional AI, usually one type or format of an output is actually created. But with advent of Generative AI, this takes the model creation and delivery to the next level. For example, as it can be seen in the above definition, many different kinds of outputs can be created which are as follows:

- Text
- Audio
- Images
- Video
- A combination of all of the above

The Cybersecurity risks of generative AI

Generative AI "caught on fire" with OpenAI, the developers and creators of ChatGPT. While the use of tools can bring many advantages to the table, it does possess its dark side as well. Examples of these include the following:

1. *Theft of Data*:
   In this case, given the sheer amount of content that ChatGPT can create in just a matter of minutes, the same can be true for creating source code on this platform. For example, if a software development team needs some new ideas or direction on where to code in their Software Development Lifecycle (SDLC), they can merely write and submit a few queries to ChatGPT, and in just a few seconds, it will give the desired outputs. It can also even be used to create source code,

but if it is a complex project, it may not be able to deliver that directly. In this regard, the Cyberattacker can also write and compile source code to create Malware. Although it is claimed that ChatGPT already has safeguards or controls in it to prevent this from happening, with some manipulation, this can be done fairly easily. One of the greatest fears is that a piece of Malware can be written that can easily heist the Personal Identifiable Information (PII) datasets, which include the likes of employees, customers, and other relevant key stakeholders. This is especially a grave risk if the entire IT and Network Infrastructure is hosted on a Cloud-based platform, such as that of the AWS or Microsoft Azure.

2. *Launching Phishing Attacks*:

   Traditional Phishing-based emails usually have telltale signs that they are not the real thing. Some of these include the following:

   - Typographical errors
   - Grammatical errors
   - Mismatches in the link that is embedded in the body of the email message versus when you hover a mouse over it
   - Odd sounding names
   - A sense of urgency to do or act on something
   - Attachments that contain a virus, such as malicious macros that are found in Excel-based spreadsheets

   An illustration of a Phishing-based email is illustrated in Figure 1.1.

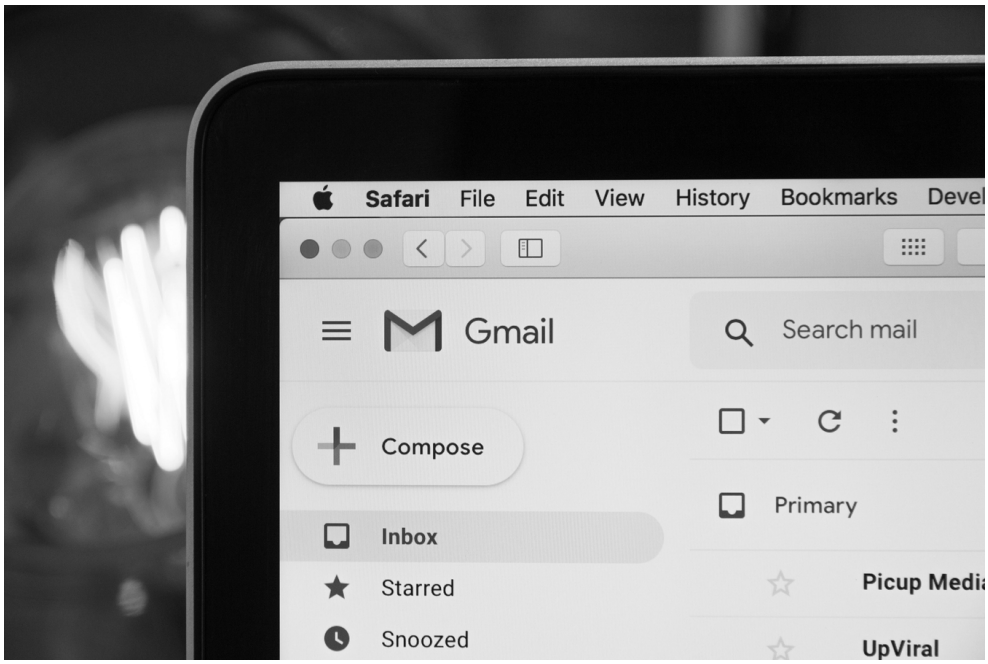


Figure 1.1 An example of a Phishing email. (Black laptop computer photo – Free Email Image on Unsplash)

But with the dawn of ChatGPT, creating a Phishing-based email without these telltale signs included in the body of the mail message, the subject line, the headers, and the sender/reply-to information can now be missing. As a result, it is now extremely difficult even for a Cybersecurity professional to discern what is real and what is not.

3. *Impersonation*:

With ChatGPT, or for that matter any model that incorporates the use of Generative AI, it is very easy now to impersonate other living people quite easily. For example, some of the outputs of ChatGPT include both audio and images, as reviewed earlier in this chapter. Thus, it is very easy to replicate the image and/or voice of a real person. As a result, these can be used in both Social Engineering Attacks and Phishing Attacks. Another variant of this is what is known

as “Deepfake”. This will be reviewed in more detail later in this chapter.

An example of an Impersonation Attack is illustrated in Figure 1.2.

Figure 1.2 An example of as Impersonation Attack. (Woman hugging man holding microphone photo – Free London Image on Unsplash)

4. *Creating Spam*:

   ChatGPT can very easily generate and create literally hundreds of Spam-based emails, which can flood the inbox of the victim in just a matter of a few seconds. Because of this, they will have to go through each email to see what is real or what is not. Worst yet, this kind of Spam-based email can be used to launch either a Denial of Service (DoS) or a Distributed Denial of Service (DDoS) Attack on a global

basis, crippling servers very quickly. As a result, gaining access to shared resources becomes very slow, if not impossible.

5. *Issues with Morality*:

   One of the greatest advantages of ChatGPT is that it can create a lot of content very quickly, no matter what it is. Because of this, many writers, authors, and content creators now make use of this platform in order to create their manuscripts. While theoretically there is nothing wrong with this, the major problem with this is that for ChatGPT to learn in order to create the optimal outputs, it must be fed a lot of data. A lot of this is content that has been previously written in the past, but others. Because of this, this work is copyrighted, and any violation of these copyrights can be easily enforced in a Court of Law. So when a writer, author, or content creator uses ChatGPT to create a manuscript, they run into the very real risk that existing content could very likely be used. As a result of this, there have been many lawsuits filed against both OpenAI and ChatGPT by the original writers, claiming that their copyrighted material has been violated, because it is being reproduced again without explicit permission being given by them.

6. *Launching Ransomware*:

   As it was just reviewed earlier, ChatGPT can be used quite easily to create source code for a piece of Malware. The same can also be said for Ransomware. The source code can be created on this platform to not only create malicious payload that will initially launch the Ransomware Attack, but ChatGPT can also be used to create both the Encryption and Decryption Algorithms that can lock and unlock the victim's files, respectively, after the Ransomware Attack has been deployed.

7. *The Use of Misinformation and Disinformation*:

There is often a great deal of confusion between the two of these, and thus, they are technically defined as follows.
Disinformation is defined as follows:

> False information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth.
>
> (Overview – Disinformation – LibGuides at MIT Libraries)

Misinformation is defined as follows:

> Misinformation is false or inaccurate information that is mistakenly or inadvertently created or spread; the intent is not to deceive.
>
> (What is "Fake News"?? – "Fake News"?," Lies and Propaganda: How to Sort Fact from Fiction – Research Guides at University of Michigan Library)

Thus, as one can see from these two definitions, the former is information and data that are used to create harm upon the victim by essentially spreading rumors, whereas with the latter, it is information and data that are simply just wrong; there is no intent to create harm with this. Obviously, the Cyberattacker will opt for creating Misinformation. Because of this, ChatGPT is a highly favored tool for doing this. Although Misinformation can be deployed and spread at any point in time, one of the most favored venues for doing this is during the Presidential Elections here in the United States. This is typically done on all of the major Social Media Platforms, especially with that of X, formerly known as Twitter. Misinformation is very

often used to launch sophisticated Social Engineering and dangerous Cyberbullying Attacks.

8. *The Cyberattacker*:
   Many people have this image that the Cyberattacker is very well versed in the tools of their proverbial trade. While this can be true, with ChatGPT and other forms of Generative AI, even a novice can now have the image of being a professional Cyberattacker. In just a matter of a short period of time, just about anybody with no experience can write and compile the source code for a malicious payload. If they don't know how to deploy it, they can easily procure the services of a true hacker and purchase their services right off the Dark Web.
9. *API*:
   This is an acronym that stands for "Application Programming Interface". It can be technically defined as follows:

> APIs are mechanisms that enable two software components to communicate with each other using a set of definitions and protocols.
>
> (What is an API? – Application Programming Interface Explained – AWS)

It should be noted that APIs are also heavily used by software developers. The primary reason for this is that creating source code from scratch can be a time-consuming and costly process. In this case, APIs already consist of source code that the software development team can modify and revise to fit the exact needs of their project requirements. Very often, they are used in web-based applications in order to bridge the front end (which is very often the Graphical User Interface, or GUI) and the backend, which is the database server. A

bulk of these are available free of charge from open-source libraries. While this is the main advantage of it, the downside of using APIs in this regard is that these open-source libraries do not often update their APIs. As a result, they can possess a lot of key vulnerabilities and weaknesses. While a Vulnerability Scanner can do this, it requires some previous knowledge to use it effectively. But to the novice wanting to break through these APIs, even using ChatGPT can provide up-to-date tips on how to penetrate them.

10. *Data Poisoning*:

    As it has been reviewed earlier in this chapter, Generative AI models, including those power ChatGPT, need a lot of data not only to train on but also to keep their algorithms optimized so that they can provide the most optimal and accurate outputs that are possible. While anybody can literally just "dump in" all of the needed datasets, they have to be optimized and cleansed first before they can be of any use to the Generative AI model. If not, the outputs will be highly skewed, providing no value whatsoever to the end user. But it is also important to keep in mind that even when these datasets are cleansed and optimized, they are still prone to being in the cross hairs of the Cyberattacker. This is known officially as "Data Poisoning"; it can be technically defined as follows:

> Data poisoning is a technique where attackers deliberately feed misleading or malicious data into the model's training set, aiming to corrupt its learning process and influence its future outputs.
>
> (https://www.exabeam.com/explainers/ai-cyber-security/chatgpt-in-the-organization-top-security-risks-and-mitigations/)

This is where the Cyberattacker will penetrate through the gaps and weaknesses of the Generative AI model and from there inject rogue datasets. Not only will this provide the wrong outputs, but it can also corrupt the model entirely, thus making it that much more prone to a Data Exfiltration Attack.

11. *Sensitive Data*:

    It should be noted that Generative AI models not just train on the datasets that are fed into them, but they can also learn from other sources as well. A prime example of this is when an end user interacts with a Digital Personality online. A great example of this is in the healthcare industry, where they are used to lead a "Virtual Appointment" with the patient, in lieu of a real live medical professional. While the patient may be led to believe that this so-called Virtual Appointment and that all information and data that are shared will be held in the strictest level of confidence, the truth of the matter is that it can be used to further train the Digital Personality and the other Generative AI models that are associated with it. Although the healthcare organization should be notifying the patient ahead of time about this, they usually are not. So this not only violates the confidentiality of a doctor–patient relationship, but it can also pose grave consequences to the healthcare organization if this confidential information and data have been breached in any way, shape, or form.

12. *Insider Attacks*:

    In the world of both Physical Security and Cybersecurity, Insider Attacks are not only some of the gravest forms of a threat variant, but they are also extremely difficult to detect until it's too late. Very often, these are done by rogue employees and/or third-party contractors, with intimate knowledge of the IT and Network Infrastructure of the

business in question. In this regard, if they also have knowledge of any kind or type of AI model (not just those that are Generative AI based), a lot of damage can happen to the organization if any of the datasets are breached, and from there, they can be sent off to the Dark Web to be sold or used to launch an Extortion Attack.

An overview into Deepfakes

One of the biggest nemeses of Generative AI is what is known as "Deepfake". It can be technically defined as follows:

> A deepfake refers to a specific kind of synthetic media where a person in an image or video is swapped with another person's likeness.
>
> (Deepfakes, explained | MIT Sloan)

A prime example of this is during the United States Presidential Elections. As the time comes closer when the two nominees are picked of both parties (Republican and Democrat), a lot of money is of course spent on all kinds and types of advertisements, in print, on television, and heavily on the Social Media Platforms. When these pieces of content are first created, they usually are genuine and are created by the respective parties.

However, the Cyberattacker can take this one step further, for very nefarious purposes. Using sophisticated Generative AI models, they can create a replica of that particular political candidate and actually use that to launch a Social Engineering and/or Phishing Attack. In this regard, a replicated video can be created and used to trick victims into donating money for that particular campaign. But instead of collected funds being used for the worthy cause, they are sent off to an offshore bank account to which only the Cyberattacker has access to.

An illustration of a Deepfake can be seen in Figure 1.3.

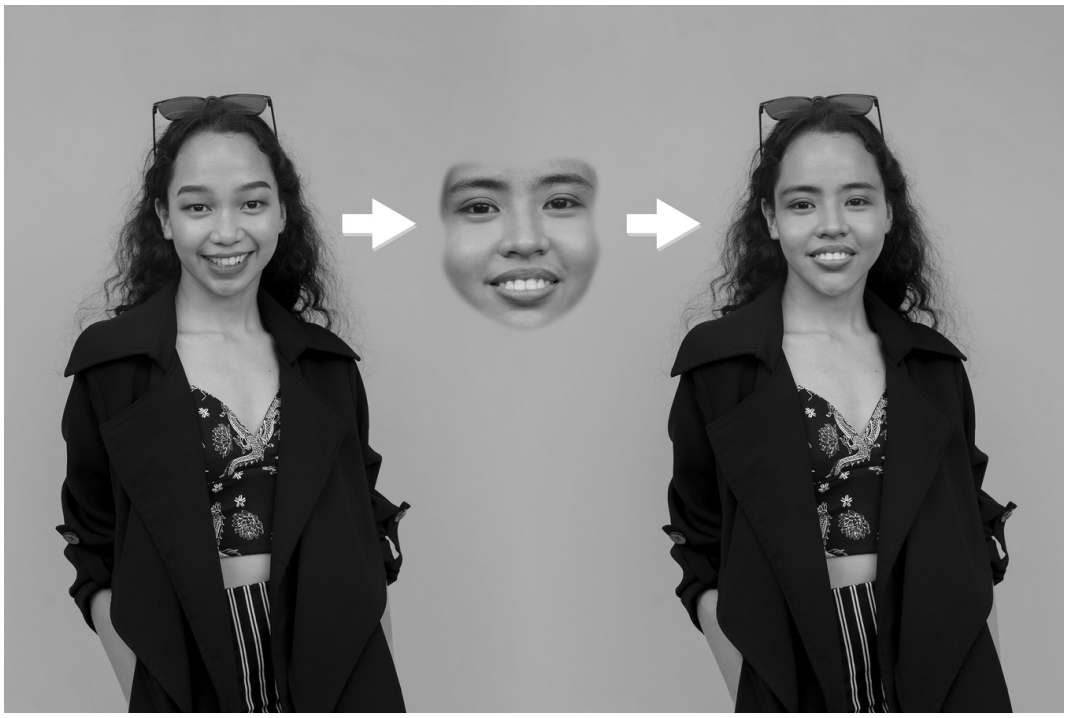


Figure 1.3 An example of a Deepfake.

As one can see from the above, the real person can be seen on the left, the replicated face that has been created making use of Generative AI is in the middle, and the Deepfake is on the right.

The science behind Deepfakes

There are two types of Generative AI algorithms that are used to create Deepfakes and are as follows:

1. *The Generator*:
   This algorithm creates and builds a large volume of training data sets on the desired output that is to be created. In this case with the Deepfakes, the training data involves the creation of the first round of fake digital content, such as the video.
2. *The Discriminator*:

This algorithm closely examines just how realistic or fake the first cut of the content actually is. It is important to note that this is purely an iterative process and is repeated over and over again until the Generator can create a very convincing fake video or image. In turn, the Discriminator will become much more "skilled" at locating any flaws that have been created for the Generator to further correct.

The culmination of both the Generator and the Discriminator yields what is known as the "General Adversarial Network", also known simply as "GAN". This is illustrated in Figure 1.4.

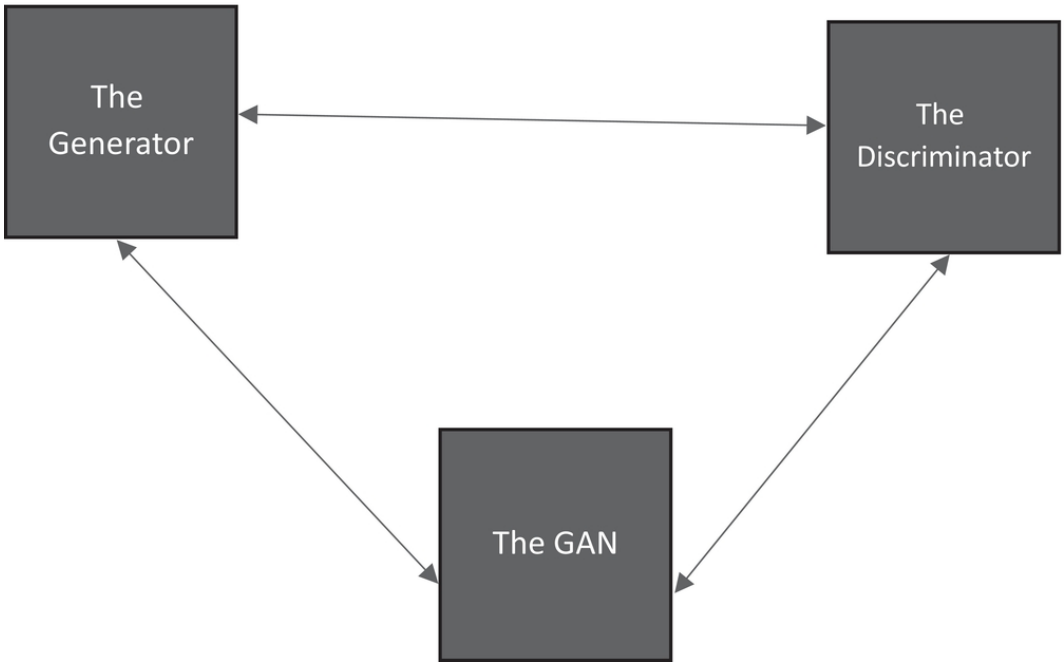


Figure 1.4 The creation of a Deepfake.

If a Deepfake video is created, the GAN then views it from different angles to analyze behavior, movement, gestures, various speech patterns, and inflections. This is then sent back to the Discriminator on an iterative basis in an effort to fine-tune the realism of the Deepfake video.

There are other technologies as well that can be used to increase the level of the sophistication of the Deepfake video, thus making it almost impossible to tell that it is not the real person. These are as follows:

1. *The CNNs*:
   This is an acronym that stands for "Convolutional Neural Networks". As its name implies, these are Neural Network-based Algorithms that can analyze all of the patterns in visual-based data. As a result, it is heavily used in Facial Recognition.
2. *The Autoencoder*:
   This is yet another type of a Neural Network Algorithm that identifies the relevant attributes of the real person such as facial expressions and body movements and then replicates them onto the Deepfake video.
3. *The NLP*:
   This is an acronym that stands for "Natural Language Processing". It is also a subset of AI, but rather than it being used to create Deepfake videos, it is used to create Deepfake audio. The algorithms of the NLP can analyze the attributes of a real person's speech and then replicate that into a very convincing, yet fake, audio clip, which once again can be used for launching Social Engineering and/or Phishing-based Attacks.
4. *The HPC*:
   This is an acronym that stands for "High Performance Computing". It can be technically defined as follows:

   > HPC is a technology that uses clusters of powerful processors that work in parallel to process massive, multidimensional data sets and solve complex problems at extremely high speeds.
   >
   > (What Is High-Performance Computing (HPC)? | IBM)

The HPC provides the technological resources that are needed to power sophisticated Generative AI applications, such as the Deepfakes. An image of an HPC infrastructure is illustrated in Figure 1.5.

Figure 1.5 An illustration of an HPC.

The other nefarious applications of Deepfakes

Apart from just the video and/or image aspect, Deepfakes can also be used for the following:

1. *Blackmail/Extortion*:
   Since it is very hard to discriminate what is real or what is not, Deepfakes can be used quite easily in order to launch Blackmail and/or Extortion Attacks, thus making the victim fall into total submission at the whim of the Cyberattacker.
2. *Customer Service*:

Deepfakes can also be used in phony customer support settings. For example, the Cyberattacker can create a spoofed website of a real and legitimate business and offer phony support services in an effort to gain the confidential information of the victim.

3. *False Evidence*:
   Deepfakes can also be used to create fake but yet convincing pieces of evidence that have the potential to be admitted into a Court of Law. If this goes unchecked, the end result will be a gross miscarriage of justice for the Defendant.
4. *Education*:
   Ever since the COVID-19 pandemic hit, the educational sector on a global basis was forced to resort to the techniques of e-Learning for students of all types and kinds. Even though the traditional brick and mortar classes have come back, the use of Chatbots or even Digital Personalities (which are an ultra-sophisticated version of the Chatbot) is used to teach online classes. Since they are available on a wide basis, especially on YouTube, a Cyberattacker can easily replicate them into Deepfakes and use that to develop a sense of rapport with the students, only to prey on their emotions but also to bait them into something horrible in the end.

How to detect a Deepfake

Believe it or not, there are very subtle clues that will give away a Deepfake, whether it is video or content based. In this subsection, we take a look at both.

From the video perspective

Here is what to look for in a Deepfake Video:

- Any kind or type of awkward positioning of the face. These can be hard to see at first glance, but after a very careful look, they will slowly become apparent.
- Any form of unnatural bodily movement. The way to tell this is to look for any kind or type of jerked gestures that do not appear to be steady.
- Any lighting or coloring either on the person or in the background that has very subtle shades of unnaturalness to them.
- If you have the ability to zoom into a video, you will know for sure that it is a Deepfake because it will look very “odd”.
- When the person is speaking, look for any kind or type of lip movements that are not synched up with the voice. Also, listen to any inconsistencies in the audio itself.
- For a real human being, it is always natural to blink, no matter what the environment the person is in. However, in a Deepfake video, the person will not blink at all.
- Look for any reflection in the eyes of the person in the video. If there are kind or type deviations, then you know for sure that it is a Deepfake.
- In a video, when a person wears their eyeglasses, there is usually some sort of reflection that varies in brightness as the person moves head up and down or to the side. But in a Deepfake video, the glare stays the same, no matter what the movement of the head is.

From the content perspective

A Deepfake does not have to be a video directly, per se. It has been used heavily so far in this chapter for ease of illustration purposes. It is important to note that a Deepfake can also appear in a written format or even in audio. With the former, some of the telltale signs are almost very similar to that of

a Phishing-based email. Here is what to look for if you ever encounter this situation:

- Any kind or type of misspellings.
- No coherent flow amongst the sentences.
- Email addresses that simply do not make any kind of sense.
- Any other written content that all of a sudden strays away from the original meaning of the overall content as a whole.

The legality of Deepfakes

This question often gets asked: “What are the steps I can take if I become a victim of a Deepfake?” Unfortunately, there is not a lot a victim can do unless they can prove direct harm was caused to them. The primary reason for this is that there is really no legal precedence for the prosecution of Deepfakes. In other words, theoretically speaking, they can still be considered to be legal. But because of the rapid development of them fueled in large part by Generative AI and the immediate harm that they can cause now, there are now several pieces of legislation which have been passed in order to help protect the victim. Some of these are as follows:

1. *The DEFIANCE Act*:
   This is an acronym that stands for “The Disrupt Explicit Forged Images and Non-Consensual Edits”. This is still pending legislation, but it will give the victim the ability to outright file a lawsuit and sue the perpetrator for large sums of money.
2. *The Preventing Deepfakes of Intimate Images Act*:
   This piece of legislation was first introduced as a bill back in May 2023. It criminalizes any non-consensual sharing of Deepfakes, no matter what kind they are. It also has further controls in it to protect

the victim from the unauthorized creation of digitally manipulated images of them.

3. *The Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks*:
   This piece of legislation is also commonly referred to as the "Take It Down Act". It is designed to make pornography that was created by Deepfakes totally illegal. Also, it makes it mandatory for all of the Social Media Platforms to take down any kind or type of Deepfakes within a 48-hour timespan if requested by the victim to do so.
4. *The Deepfakes Accountability Act*:
   Under this piece of legislation, all Deepfakes that have been created must have a Watermark embedded into them stating explicitly that whatever is being viewed is an actual Deepfake. Also, there are controls in place that would make the use of Deepfakes illegal if they are used in cases of Election Interference or any other kind or type of criminal-based activity.

The history of Cybersecurity

So far in this chapter, we have provided an extensive overview of some of the major Cybersecurity threat variants that are prevalent today. While some of these are old, like Phishing, many of the newer ones have been brought on by Generative AI. So at this point, it only makes sense to provide a review into the actual history of Cybersecurity and how it all got started to where it is now today. This is examined in detail in this section.

- *The 1940s*:
  - In 1945, the first digital computer known as the "ENIAC" or "Electronic Numerical Integrator and Computer" was launched.

    - The first thoughts that a mechanical organism would be able to copy and replicate itself into new hosts were conceived by Jon von Neumann. This thinking was published in a scientific paper called the “Theory of Self Reproducing Automata”.
- *The 1950s*:
    - During this, the phenomenon called “Phone Phreaking” came out. It was not a threat variant per se but rather a way to hijack the telephone protocols that existed at the time in order to make cheaper or no-cost calls.
    - The first security controls were deployed, which were mostly for Physical Access Entry, mainly for access to computers; you could reasonably lock a door and be fairly sure no one was going to tamper with a computer in that room. But the notion of computers networked together was not yet conceived.
    - By the late 1950s, the first use of Password Systems came about. But at this time, there are no standardized protocols yet available.
- *The 1960s*:
    - This is the timeframe when true hacking attempts became apparent. The first one happened in 1967, when IBM had asked college-level students to test their new computing system. From this specific experience, IBM actually learned quite a bit about what real computer-based vulnerabilities are. As a result, this gave serious rise to the concerns about security measures and protocols.
    - Despite the above, the main concerns were over the physical security of the hardware of the computer systems and preventing unauthorized access to them. The concept of Cybersecurity still did not come about yet.

    - By the late 1960s, mainframe computers became much more predominant. Because of this, the security issues that were associated with them began to emerge. And, as computers became smaller and cheaper, this focus only grew more intense in nature.
- *The 1970s*:
    - This is the era of the birth of Cybersecurity. This came about as the Advanced Research Projects Agency Network, also known as the "ARPANET", was launched in September 1969. Then many years later, the world's first operational packet-switched network came about, which was the catalyst for the first true Internet. The primary objective of this was to give end users the ability to access shared resources across the Mainframe Network, primarily across the world of academia.
    - By the mid-1970s, the first true Computer Virus came about. It was created by a person named Bob Thomas, and it replicated itself throughout the APRANET terminals that carried this message: "I'M THE CREEPER: CATCH ME IF YOU CAN".
    - In response to the above, a person by the name of Ray Tomlinson developed the counter to the first virus, known as the "Reaper, to catch Creeper". So now, the first true virus and the first true anti-virus were born.
    - As a result of the above, the United States Federal Government suddenly woke up and discovered that it had to find a way to mitigate these risks. Thus, the Advanced Research Projects Agency, a division of the Department of Defense (DoD) were born.
    - In 1979, a 16-year-old boy named Kevin Mitnick launched a Hacking Attack known as the "Ark". This was a computer system

that was created by the Digital Equipment Corporation (also known as the “DEC” for the development of the RSTS/E Operating Systems) and illegally made copies of it, which were also distributed to others as well. This was deemed to be the first true Social Engineering Attack, by the upper-level managers who gave him employee credentials. As a result, he was later the first Cyberattacker to be arrested and found guilty in a Court of Law.

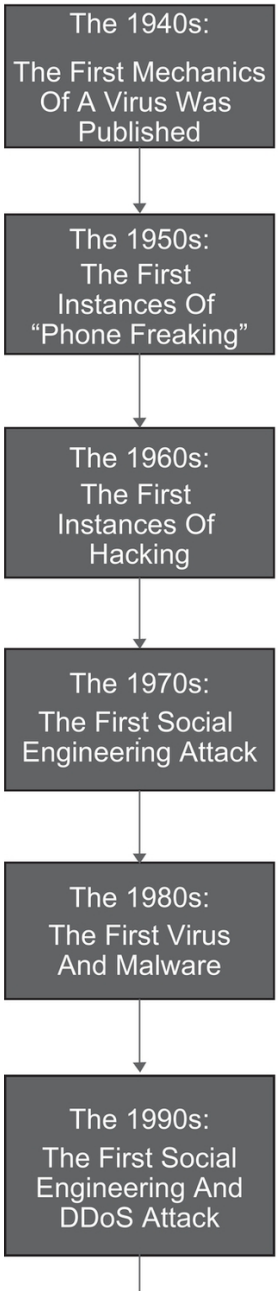
- *The 1980s*:
    - The early 1980s saw the evolution of what is known as the “Bulletin Board Systems” or “BBS” for short. This allowed for the end users to connect their personal computers to a host system, such as a server, via a modem. But as sharing resources became easier, security risks quickly came on the scene.
    - By the mid-1980s, the first pieces of Viruses and Malware appeared. Examples of these include the following:
        - The Elk Cloner Virus that targeted Apple II computers.
        - The Brain Virus that affected IBM PC systems.
        - The Morris Worm, deemed to be one of the first pieces of Malware.
    - The Domain Name System, also known as the “DNS”, which made accessing websites much easier and more automated. But passwords were still the primary means of access control, increasing the risk of vulnerabilities occurring.
    - The first true Ransomware Attack, when an infected floppy disk was given to attendees of the World Health Organization’s AIDS conference. The program was launched by Joseph L. Popp, who was subsequently arrested and charged with various counts of blackmail.

- *The 1990s*:
    - There was a continuing growth into the development and usage of digital technologies as well as the dawn of the World Wide Web. As a result, the Cybersecurity challenges also rose.
    - The first cases of Social Engineering and Distributed Denial of Service (also known as “DDoS”) Attacks. This was triggered by the popularity of Internet Relay Chat (also called “IRC”) and America Online (“AOL”).
    - The roll out of Windows 95 also garnered the attention of Cyberattackers.
    - The Electronic Frontier Foundation became the de facto entity in pushing leading discussions about the need for regulations and legislation to protect Personal Identifiable Information (PII) datasets.
    - As a result of all of the above, the late 1990s saw the birth of true Cybersecurity.
- *The 2000s*:
    - The iPod gave rise to the global adoption of the Broadband Internet, which lead to a much greater amount of increased connectivity.
    - During this time, there was also a huge uptick in the number of sophisticated pieces of Malware which were coming out. As a result, Worms, Viruses, and Trojan Horses became a lot more stealthier and harder to detect. Examples of these include the Code Red and the Nimda Worms.
    - As mobile devices and Cloud-based adoption became more prevalent, unauthorized access and data breaches became real

Cybersecurity threats. Other issues included the Shared Responsibility Model, especially for Public Cloud Deployments.
    - Because of the above, the Cybersecurity Industry started to blossom into full swing. The largest demands were for Antivirus Software, Firewalls, and Network Intrusion Detection Systems and other related security tools.
- *The 2010s*:
    - During this timeframe, there was a significant evolution with regards to the Cyber Threat Variants. For example, there was a huge transition from just Password Attacks to physical destruction of anything that the Cyberattacker could get their hands on.
    - Examples of the above included the Stuxnet worm, which was a joint United States–Israeli operation to decimate Iran's nuclear facilities, and the Snowden Leaks, which exposed a global surveillance network. Both of these events triggered the new era of Cyber Espionage.
    - The decade also saw a significant increase in both financially motivated Cybercrimes and destructive Malware being deployed, rendering entire IT and Network Infrastructures completely inoperable.
- *The Present*:
    - Cyberattacks have now become much dangerous than ever before; a lot of this has been fueled by the emergence of Generative AI. Examples of these include the following:
        - Advanced Persistent Threats.
        - Attacks launched by Nation State Actors, such as Russia, China, Iran, and North Korea.

- Ransomware Attacks that now include Extortion-based Attacks.
- Attacks to the Critical Infrastructure in the United States.
- Deepfakes, as reviewed extensively earlier in this chapter.
- Social Engineering Attacks.

The above timeline is illustrated in Figure 1.6.



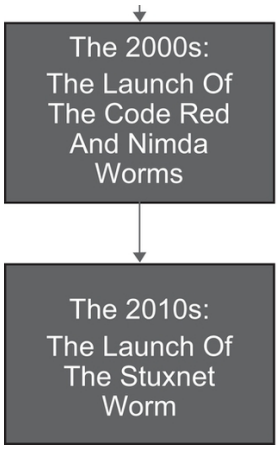


Figure 1.6 An illustration of the history of Cybersecurity.

As Cybersecurity evolved over time to where it is now, there are four major groupings of it, which are as follows:

1. *The Network Security*:
   This deals with the protection of the Network Infrastructure using tools such as Firewalls, Intrusion Detection and Prevention Systems, Virtual Private Networks (also known as "VPNs"), Routers, Log Filtering, etc.
2. *The Information Security*:
   This focuses primarily upon the Confidentiality, Integrity, and Availability (also known as the "CIA Triad") of any business. The controls that are used here include Encryption, Two Factor Authentication, Multifactor Authentication, Data Backups, etc.
3. *The Application Security*:
   This focuses primarily upon the security of software and applications, particularly those that are Web based. This is usually done by identifying and mitigating vulnerabilities that could be exploited by the Cyberattacker.
4. *The Endpoint Security*:
   This involves securing individual devices like smartphones and tablets by making use of Endpoint Detection and Response (also known as

"EDR") solutions and Mobile Device Management (also known as "MDM") tools.

Getting into the mindset of the Cyberattacker

So far in this chapter, we have reviewed some of the major Threat Variants that exist in Cybersecurity, as well as we have provided an in-depth review of its history to where it is at now. Not surprisingly, over the course of time, the Threat Variants have not only gotten stealthier, but they are now even very difficult to detect. Because of this, it is very important to get into the actual mindset of the Cyberattacker and try to figure out how they plan and launch their Threat Variants.

This is very much needed, especially for both Penetration Testing, Vulnerability Scanning, and Threat Hunting exercises. Even though the common denominator between all of three of these is to find the weaknesses, gaps, and vulnerabilities in an IT/Network Infrastructure, they all have subtle differences amongst them and are reviewed in more detail into the next subsections of this chapter.

Penetration Testing

This can be technically defined as follows:

> A penetration test, or "pen test," is a security test that launches a mock cyberattack to find vulnerabilities in a computer system. Penetration testers are security professionals skilled in the art of ethical hacking, which is the use of hacking tools and techniques to fix security weaknesses rather than cause harm. Companies hire pen testers to launch simulated attacks against their apps, networks, and

> other assets. By staging fake attacks, pen testers help security teams uncover critical security vulnerabilities and improve the overall security posture.
>
> (What is Penetration Testing? | IBM)

Penetration Testing is actually a very large field, and the exercises that are conducted from within it are actually complex. They can be done on site, or even virtually, from many thousands of miles away. They can also be fully automated, be done manually, or even be a hybrid of both. Typically, the Penetration Testing team is divided into three main groups, which are as follows:

- *The Red Team*:
  These are the Penetration Testers that will take an offensive role and make an attempt to break down the walls of defenses in order to find any of the gaps, vulnerabilities, and weaknesses.
- *The Blue Team*:
  These are the Penetration Testers that work in concert with the IT Security team. The objectives are twofold:
  - To counter the offensive moves that are made by the Red Team.
  - To provide further training, insight, and knowledge to the IT Security team as to how they can improve the security posture of the business that is tasked with defending.
- *The Purple Team*:
  These are the Penetration Testers from both the Red Team and the Blue Team. Together, the Purple Team serves as a counter-balance to ensure that the exercises are conducted in the best interests of the client and that it is being done as objectively and unbiased as possible. Finally,

the Purple Team is tasked with compiling the final report to the client, after all of the Penetration Testing exercises have been completed.

An illustration of Penetration Testing is shown in Figure 1.7.

Figure 1.7 An illustration of Penetration Testing.

It is important to note that Penetration Testing is now technically referred to as “Ethical Hacking”. This can also be technically defined as follows:

> Ethical hacking is an authorized attempt to gain unauthorized access to a computer system, application, or data using the strategies and actions of malicious attackers. This practice helps identify security vulnerabilities that can then be resolved before a malicious attacker has the opportunity to exploit them.
>
> (What Is Ethical Hacking and How Does It Work? | Black Duck)

So, although the Penetration Testing team is taking the approach, mindset, and tactics of the Cyberattacker, whatever tests are being done are conducted from within the bounds of the Law. In this regard, both the client and the Penetration Testing have to sign a legal contract, which stipulates that the client has given explicit permission to penetrate the targets and are

both fully aware and cognizant of the risks of conducting these kinds of exercises.

But it could be the case that the Penetration Testing team would like to select some newer targets in order to get a full picture of the Cyber Threat Landscape the client faces. They simply cannot choose at the whim and hit upon newer assets. Just like before, they have to get explicit permission (and written) before they can move forward with penetrating into these newer targets.

Vulnerability Scanning

Vulnerability Scanning is yet another alternative to Penetration Testing. It can be technically defined as follows:

> Vulnerability scanning is the process of discovering, analyzing, and reporting on security flaws and vulnerabilities. Vulnerability scans are conducted via automated vulnerability scanning tools to identify potential risk exposures and attack vectors across an organization's networks, hardware, software, and systems.
>
> (https://www.beyondtrust.com/resources/glossary/vulnerability-scanning)

While Vulnerability Scanning can be an effective tool used to find the gaps and weaknesses in an IT and Network Infrastructure, there are some key differences when compared to Penetration Testing. Some of these are as follows:

Vulnerability Assessment	Penetration Test
Tests are passive	Tests are active
Tests are automated, no human intervention	Tests are primarily manual, lots of human intervention
Tests are short in time frame	Tests are much longer in time frame
Reports are provided to the client, but not specifically for actions that can remediate issues	Reports are provided to the client and are specific to actions that remediate specific issues
Scans can be run on a continual cycle	Scanning is done only at a point in time intervals due to their exhaustive nature
Tests are primarily done on digital assets	Tests are done on both physical and digital assets
Only known vulnerabilities are discovered	Both known and unknown vulnerabilities are discovered
Costs are affordable	Costs can be quite expensive
Only general tests are done	All kinds of tests are done, depending upon the requirements of the client

But the key difference between the Penetration Test and the Vulnerability Scan is that the former is considered to be an “Active Scan” and the latter is considered to be a “Passive Scan”. They both can be technically defined as follows:

- *The Active Scan*:

  Also known as standard asset discovery, active asset discovery is a method of monitoring IT assets by examining their traffic and

examining the IT environment. Using this method, it is possible to determine different types of devices using an IP address (such as an operating system or vulnerability).

(Active vs passive scanning in IT environments | Virima)

- *The Passive Scan*:

  Passive scanning is what happens when a vulnerability scanner runs on a network and detects assets. It's the most common type of asset discovery, but it has some limitations.

  (Active vs passive scanning in IT environments | Virima)

As one can see, the Penetration Test is a very comprehensive exercise. It examines certain targets, provided that there is explicit consent from the client, as just reviewed earlier. It does a deep dive into each one, determining *all of the weaknesses and gaps in them*, whereas with the Vulnerability Scan, it can literally scan the entire IT and Network Infrastructure. While this sounds very advantageous, this is just a cursory check of all of the digital assets. *It does not do a deep dive into each one of them*. Vulnerability Scans are primarily used for determining which of the Network Ports have remained open and have gone unnoticed over a period of time.

These of course are primary entry points for the Cyberattacker to enter into. Also, like the Penetration Test, a final report is prepared for the client describing what has been discovered and the remediations for them. The main drawback to this is that the client is very often left to reviewing the material themselves, unless they get the help of an Managed Service Provider (MSP) or an Managed Security Services Provider (MSSP) to interpret the findings. But one of the two main advantages of the

Vulnerability Scan is that it is much cheaper when compared to the actual cost of doing a Penetration Test, and it is done on an automated basis.

An example of Vulnerability Scanning is illustrated in Figure 1.8.

Figure 1.8 An illustration of Vulnerability Scanning.

Threat Hunting

Another option that is available to the Chief Information Security Officer (CISO) and their respective IT Security team is that of the Threat Hunt. It can be technically defined as follows:

> Threat hunting is the practice of proactively searching for cyber threats that are lurking undetected in a network. Cyber threat hunting digs deep to find malicious actors in your environment that have slipped past your initial endpoint security defenses.
>
> After sneaking in, an attacker can stealthily remain in a network for months as they quietly collect data, look for confidential material, or obtain login credentials that will allow them to move laterally across the environment.
>
> (What Is Cyber Threat Hunting? [Proactive Guide] | CrowdStrike)

Threat Hunting involves key three steps, which are as follows:

1. *A Trigger*:
   This is an event or even an alert or warning that points the Threat Hunters to a specific area in the Network Infrastructure that requires further investigation. Further discovery could very well indicate that Malicious Activity is underway.
2. *An Investigation*:
   The Threat Hunting team uses technology such as EDR (Endpoint Detection and Response) to take a detailed look into the Malicious Compromise of the IT and Network Infrastructure. This phase of the Threat Hunt will keep going on until the event is determined to be benign or until a complete and comprehensive picture of the Malicious Behavior has been created.
3. *A Resolution*:
   This last phase involves communicating about what has been discovered to the relevant stakeholders so that appropriate action can be taken to appropriately respond to the incident and to mitigate any further threats that could arise from the Malicious Activity that was found by the Threat Hunting team. From this point onwards, the data and intelligence that have been gathered can be inputted into automated technology platform (such as those are powered by Generative AI) to improve future processes and operations.

In this entire process, the Cyber Threat Hunting team will gather as much information and data about the Cyberattacker's actions, methodologies, and goals. Threat Intelligence is also gathered, to in attempt to predict the Signature Profiles of potential Threat Variants.

It is very important to note here that Threat Hunting is primarily involved with examining the internal aspects of the IT and Network Infrastructure, primarily to determine if a Cyberattacker is lurking covertly from within

this domain, as the above definition clearly describes. Finally, an image of Threat Hunting is shown in Figure 1.9.

Figure 1.9 An illustration of Threat Hunting.

The methodologies of the Cyberattacker

So far in this chapter, we have covered the following:

- Some of the major Cyber Threat Variants.
- A chronological overview into the evolution of Cybersecurity.
- The tools that are available to detect and mitigate the Cyber Threat Variants, which include the following:
    - Penetration Testing
    - Vulnerability Scanning
    - Threat Hunting

At this stage in this chapter, it is very important to look at some of the methodologies as to how the Cyberattacker actually plans their moves. We start first with the MITRE ATT&CK Model.

The MITRE ATT&CK Model

The MITRE ATT&CK framework was originally created and deployed by the MITRE Corporation all the way back in 2013 and was a culmination of

the Fort Meade Experiment, also known as the “FMX”. The key question that was being asked was and continues to be is as follows:

> How well are we doing at detecting documented adversary behavior?
>
> (What Is the MITRE ATT&CK Framework? | Get the 101 Guide | Trellix)

It is an acronym that stands for *A*dversarial *T*actics, *T*echniques, *and C*ommon *K*nowledge. It is a knowledge base or repository that reflects the actual behavior the Cyberattacker intends to take when they launch their specific threat variant. It demonstrates the actual thought process or the lifecycle that they go through to plan out how they will penetrate the IT/Network Infrastructure of a business.

The components of the MITRE ATT&CK Framework

There are three major components to the MITRE ATT&CK framework, and they are as follows:

1. *The Tactics*:
   These are the short-term goals that the Cyberattacker wishes to achieve when they launch their threat variant.
2. *The Techniques*:
   These are the methodologies in which the Cyberattacker will reach their objectives, through launching and deployment of their specific threat variant.
3. *Documentation*:
   These are the actual methodologies or techniques that all kinds of Cyberattacker have used in the past to launch and deploy their specific threat variants.

You can view this in more detail at this link:

MITRE ATT&CK®

It is important to note the following:

- The columns represent the Tactics.
- The techniques that the Cyberattacker uses are the individual cells in each column.
- The actual methodologies that have been used by the Cyberattacker are linked from the techniques, and they are highlighted in yellow in the above illustration.

The techniques of the MITRE ATT&CK Framework

The techniques from the illustration are detailed below:

1. *Reconnaissance*:
   This is where the Cyberattacker scouts out and attempts to gather intelligence about the IT/Network Infrastructure of the target.
2. *Resource Development*:
   This is the phase in which the Cyberattacker establishes the resources that they will need to launch their specific threat variant. For example, this could be a Command-and-Control Center, in which actions can be conducted remotely. This will also make the Cyberattacker invisible to the outside world.
3. *Initial Access*:
   The Cyberattacker now tries to get their first foothold into the IT/Network Infrastructure of the business. This can be done by numerous ways, which include the following:
   - Phishing

- Ransomware
- Social Engineering
- Source Code Exploitation
- Trojan Horses
- Any other kind or type of Malicious Payload, especially those created by Generative AI.

4. *Execution*:
   This is where the Malicious Payload is activated by the Cyberattacker. This is very often done remotely, through the Command-and-Control Center that was created in Step #2.
5. *Persistence*:
   In this phase, the Cyberattacker attempts to stay into the IT and Network Infrastructure of the business, without being noticed. They also make attempts to move across, in a lateral-based fashion.
6. *Privilege Escalation*:
   Once the Cyberattacker has made enough points of entry, one of their main objectives is to go after the proverbial "Crown Jewels", namely the passwords of the employees. In this regard, one of the most sought-after targets is Privileged Managed Account, which represents the super user passwords.
7. *Defense Evasion*:
   The Cyberattacker tries to cover their tracks to a greater extent. This is often accomplished by deploying the malicious payload into the CPU and the memory areas of the device. These are often referred to as "Fileless Attacks".
8. *Credential Access*:
   At this phase, once the Cyberattacker has acquired their initial "Crown Jewels", they will now make the attempt to be much more daring and

try other techniques to get to other digital assets. An example here would be to deploy a Keylogger that can record the keystrokes of employees. Not only with they be able to gain additional passwords with this, but they can even build up a profile about their targeted victim.

9. *Discovery*:
   As the Cyberattacker penetrates deeper into the IT and Network Infrastructure of the business, they will now attempt to scope out other parts of it. This will include the Servers, Databases, Intellectual Property, and even the physical assets.
10. *Lateral Movement*:
    This was examined in Step #5. At this point, the Cyberattacker will review the lateral movements that they have used before and further optimize them.
11. *Collection*:
    Once the Cyberattacker has gained access to some of the "Crown Jewels", they will now make the attempt to try to gain access to other prized possessions from other sources, such as a Private Cloud, Hybrid Cloud, or even in different areas of an On Premises IT and Network Infrastructure.
12. *Command and Control*:
    This was also reviewed in Step #2. Once the first Command and Control Center has proven to be successful, they will then, at this point, attempt to replicate more of them. This is an effort to launch multiple attacks towards the IT and Network Infrastructure of the business. A prime example of this is Distributed Denial of Service (DDoS) attack. Multiple Command and Control Centers are deployed to target hundreds, if not thousands, of servers all at once.

13. *Exfiltration*:
    The Cyberattacker will now attempt to hijack the Personal Identifiable Information (PII) datasets of customers, employees, and other key stakeholders. The primary goal here is not to steal them all at once, but a bit at a time, so that the business will not realize this until it is too late.
14. *Impact*:
    This is the very last phase of the framework. At this point, once the Cyberattacker has collected all the "Crown Jewels" that they can, the final goal now is to cause as much damage as possible towards the business. This could be launching a Ransomware Attack, selling the PII datasets on the Dark Web or even using them to launch an Extortion Attack.

The three models of the MITRE ATT&CK Framework

At the present time, there are four different models of the MITRE ATT&CK framework. They are as follows:

1. *The Enterprise Matrix*:
   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Enterprise Infrastructure. This is all inclusive model that covers the following:
   - Windows Platforms
   - Linux Platforms
   - MacOS Platforms
   - Any kind of IT and Network Infrastructure
   - Any kind of Cloud Platforms (such as the AWS and Microsoft Azure)
   - All kinds of Containers

2. *The Mobile Matrix*:
   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Mobile Infrastructure, such as those devices that make use of the iOS and Android Operating Systems.
3. *The ICS Matrix*:
   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Critical Infrastructure that makes use of Industrial Control Systems. Examples of this include nuclear facilities, the national power grid, the food distribution system, oil and gas pipelines, and the water supply. There is a special emphasis here on the sensors and networks that enable automation.
4. *The Cloud Matrix*:
   This model focuses upon the motives, intentions, and techniques of the Cyberattacker as it relates to the Cloud Deployments, most notable of the Google Cloud Platform (GCP), the AWS, and Microsoft Azure.

The use cases of the MITRE ATT&CK Framework

The question at this point often gets asked is: “How can one use the MITRE ATT&CK framework”? Here are some actual use cases:

1. *Emulation*:
   Along with using tools such as Generative AI, the framework can also be used accurately to predict what a Cyberattacker could potentially do in the future. From this, various “what if” scenarios can be created.
2. *Penetration Testing*:
   Given the breadth and scope of the framework, it can also be quite applicable to the Red Team, as they try to get into the mindset of a Cyberattacker when they do their Penetration Testing exercises.
3. *Behavioral Patterns*:

Since the core of the framework is centered around understanding the intent and motives of the Cyberattacker, it can also be used to help create a profile of their behavioral patterns.

4. *Risk Assessment*:
   To varying degrees, the framework can also be used by the CISO and their IT Security team to gauge the degree of vulnerability of both the physical and digital assets that their business contains.
5. *SOC*:
   This is an acronym that stands for the "Secure Operations Center". In this regard, the framework can also be used to see just how responsive the team that operates this is in detecting and responding to a threat variant.
6. *Threat Hunting and Research*:
   The framework can also give a wealth of information and knowledge not only to Threat Hunters but also to Threat Researchers, as they model future attack vectors based on previous signature profiles.

An application of the MITRE ATT&CK Framework: Microsoft 365

The MITRE ATT&CK framework is a very well-established and widely used methodology to map out in detail how the Cyberattacker will launch their next threat variant.

Many companies have and are continuing this framework. A great example of this is Microsoft and how they deployed the M365 subscription. In this regard, the following offerings are mapped to the MITRE ATT&CK framework:

1. *Microsoft 365 Defender, XDR, and Office 365*:

This is an all-encompassing security mechanism that does the following:

- Detection
- Prevention
- Investigation
- Response to all the identities, tenants, email, and all software applications that reside in M365 subscription.

2. *Microsoft Entra ID*:
   This is formerly known as Azure Active Director or AAD for short. It is primarily available in Microsoft Azure and uses the concepts of the MITRE ATT&CK framework to provide Identity and Access Management (also known as IAM) services to manage employee profiles, and the rights, privileges, and permissions that they must access the resources from within Microsoft Azure.
3. *Microsoft Exchange Online Protection*:
   This is a package that provides all kinds of protection from emails coming in or out of Microsoft Exchange. This includes the following:
   - Spam
   - Malware
   - Phishing
   - Other threats variants, such as rogue attachments and malicious links.
4. *Microsoft Purview*:
   This is a governance platform that comes with most M365 subscriptions. By following the concepts of the MITRE ATT&CK framework, any business can come into compliance with the major data privacy laws of the GDRP, CCPA, HIPAA, etc.

The Lockheed Martin Cyber Kill Model

This is yet another framework that was developed by the Lockheed Martin Corporation, back in 2011. It is actually yet another iteration of the United States Military Kill Chain, which is a step-by-step methodology that is designed to locate, identify, and stop enemy activity right in its tracks. It has been and continues to be applied to the following Cyber Threat Variants:

- Malware
- Ransomware
- Trojan Horses
- Spoofing
- Social Engineering
- Advanced Persistent Threats (also commonly known as the "APTs").

The last Threat Variant can be technically defined as follows:

> An advanced persistent threat (APT) is a covert cyber attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period. During the time between infection and remediation the hacker will often monitor, intercept, and relay information and sensitive data.
>
> (What Is an Advanced Persistent Threat (APT)? – Cisco)

A simple example of this is illustrated in Figure 1.10.

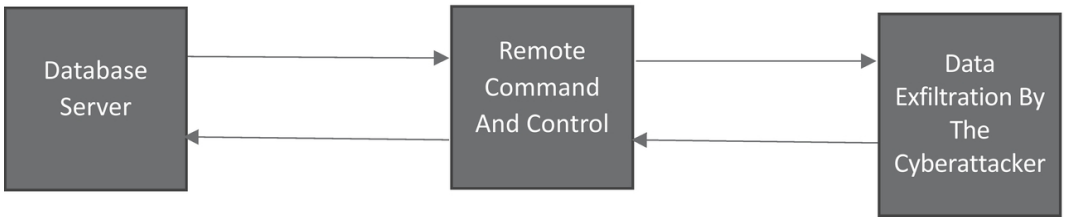


Figure 1.10 An illustration of an Advanced Persistent Threat (APT).

In the above, the Cyberattacker can easily penetrate the Database Server via a Command and Control Center. This is typically used by them, in order to cover their tracks and go unnoticeable, such as by masking their IP Address. From their remote location, the Cyberattacker can then launch a Data Exfiltration Attack against the Database Server and heist all kinds and types of Personal Identifiable Information (PII) datasets of employees, customers, and key stakeholders of the targeted business.

The eight phases of the Lockheed Martin Cyber Kill Model

Just like the MITRE ATT&CK framework, the Lockheed Martin Cyber Kill Chain Model consists of eight distinct steps, which are as follows:

1. *The Reconnaissance*:
   In this first phase, the Cyberattacker first identifies the digital asset(s) that are to be targeted. From here, they then explore all of the vulnerabilities and weaknesses that can be exploited. Activities here include the following:
   - The harvesting of login credentials
   - Gathering email addresses
   - The physical locations of any On Premises Servers and their respective software applications and Operating System (OS) details.
2. *The Weaponization*:
   In this second phase, the Cyberattacker develops their Threat Vector, which is most likely a nefarious piece of Malware, which can be used in a Ransomware Attack. Also, the Cyberattacker could also set up other unknown backdoors to be used as covert Point of Entry in case their first one is discovered and shut down by the Network Administrator.

3. *The Delivery*:
   In this third phase, the Cyberattacker launches the Malicious Payload. Also, they may use Social Engineering techniques to increase the effectiveness of the security breach.
4. *The Exploitation*:
   In this fourth phase, the Malicious Payload is deployed onto the targeted Digital Asset(s).
5. *The Installation*:
   In this fifth phase, the Malicious Payload is now activated or triggered. This can be deemed as the turning point in the model, as the Cyberattacker has now made the first penetration into the IT and Network Infrastructure of the system and can now gain full and complete control of the targeted Digital Asset(s).
6. *The Command and Control*:
   In this sixth phase, the Cyberattacker can utilize the Malicious Payload to also assume Remote Control of the targeted Digital Asset(s). Also, the Cyberattacker can also move in a lateral fashion throughout the IT and Network Infrastructure.
7. *The Actions on the Objectives*:
   In this seventh phase, the Cyberattacker now carries and executes their intended goals, with one of the main ones being that of Data Exfiltration or launching Ransomware Attacks.
8. *The Monetization*:
   In this eighth phase, the Cyberattacker attempts to make a profit from their recent security breach. This typically involves the selling of the Personal Identifiable Information (PII) datasets onto the Dark Web.

All of these eight distinct phases are illustrated in Figure 1.11.

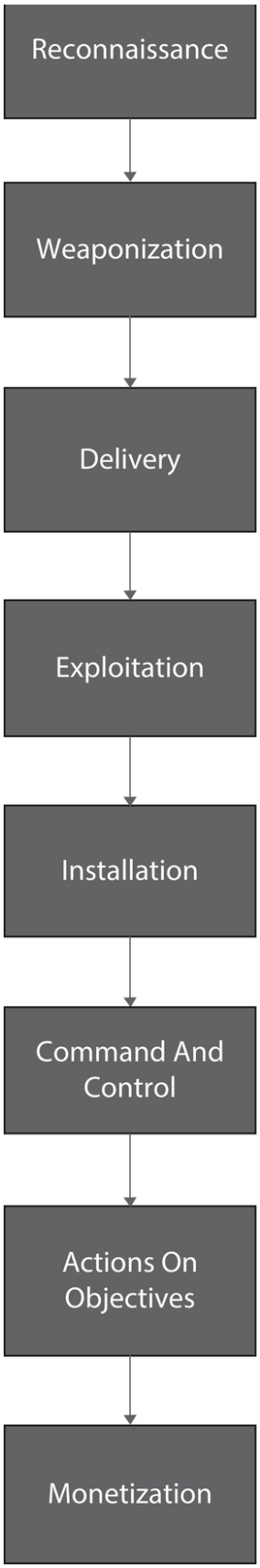

Reconnaissance
Weaponization
Delivery
Exploitation
Installation
Command And Control
Actions On Objectives
Monetization

Figure 1.11 An illustration of Kill Chain Model.

The drawbacks of the Lockheed Martin Cyber Kill Model

1. *The Focus on Perimeter Security*:
   Perimeter Security can be technically defined as follows:

   > In essence, perimeter security is as it says, a defense system around your network designed to stop external threats from entering. Imagine your internal network as a castle; your perimeter network security consists of the weapons you'd put in place atop and around the castle (canons, archers, etc.) to defend from invaders – in this case, network threats.
   >
   > (Perimeter Security Basics And Why We Need It – Netcentrix)

   Although the Perimeter Security Model has been used for decades, it is starting to get outdated for one simple reason: Given the advanced Threat Variants of today, if the Cyberattacker can break through the perimeter in one fell swoop, they will have access to all of the Digital Assets in the IT and Network Infrastructure. In other words, there is only one true line of defense, and if it is broken, complete access can be gained. As a result of this, many businesses of today are now opting for the what is known as the "Zero Trust Framework". This is where the IT and Network Infrastructure is divided into different segments or "zones", with each one of them having at least three or more layers of defense. Thus, if the Cyberattacker were to break through one of them, the chances of them breaking through all of the zones decreases to an almost statistical zero. However, the Lockheed Martin Cyber Kill Chain Model cannot be used here.
2. *The Attack Detection*:

Another huge shortcoming of the Lockheed Martin Cyber Kill Chain Model is that it cannot be used to detect Insider Threats, which is amongst the most serious Cyber Risks to a business, and because of that, it has one of the highest rates of success. It also cannot be used to detect Cross Site Scripting (also known as "XSS"), SQL Injection Attacks, Distributed Denial of Service (also known as "DoS"), Distributed Denial of Service (also known as "DDoS") Attacks, and Zero Day Exploits.

3. *The Highly Researched Attacks*:
   It should be noted that the Lockheed Martin Cyber Kill Chain Model is only effective when the Cyberattacker does a lot of manual research into their intended target(s). But with the advent of Generative AI, automation is now being used, which is something that the Model simply cannot address.

The Diamond Model of Intrusion Analysis

This is yet another framework that has been created in an effort to not only understand the tactics of the Cyberattacker but to try to understand their behavior as well. What makes this framework different from the MITRE ATT&CK Framework and the Lockheed Martin Cyber Kill Chain Model is that there are four distinct components to it, and the goal is to study the interaction amongst all of them. So, it does not take an incremental/progressive like the other two model/framework does.

The framework was first developed by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz in 2013. It was published in a technical report titled "The Diamond Model of Intrusion Analysis".

The four components are as follows:

1. *The Adversary*:

This is the actual Cyberattacker and/or their group that is going to or has already launched the Threat Variant.

2. *The Infrastructure*:
   These are the technical-based resources that the Cyberattacker makes use of to not only create the Threat Variant but to also deploy and execute it. This can range from the Servers to Domains to the IP Addresses.
3. *The Capability*:
   This is the methodology and the technique that the Cyberattacker uses during the actual security breach.
4. *The Victim*:
   This is the intended target of the Cyberattacker, whether it is physical or physiological.

These four components are illustrated in Figure 1.12.

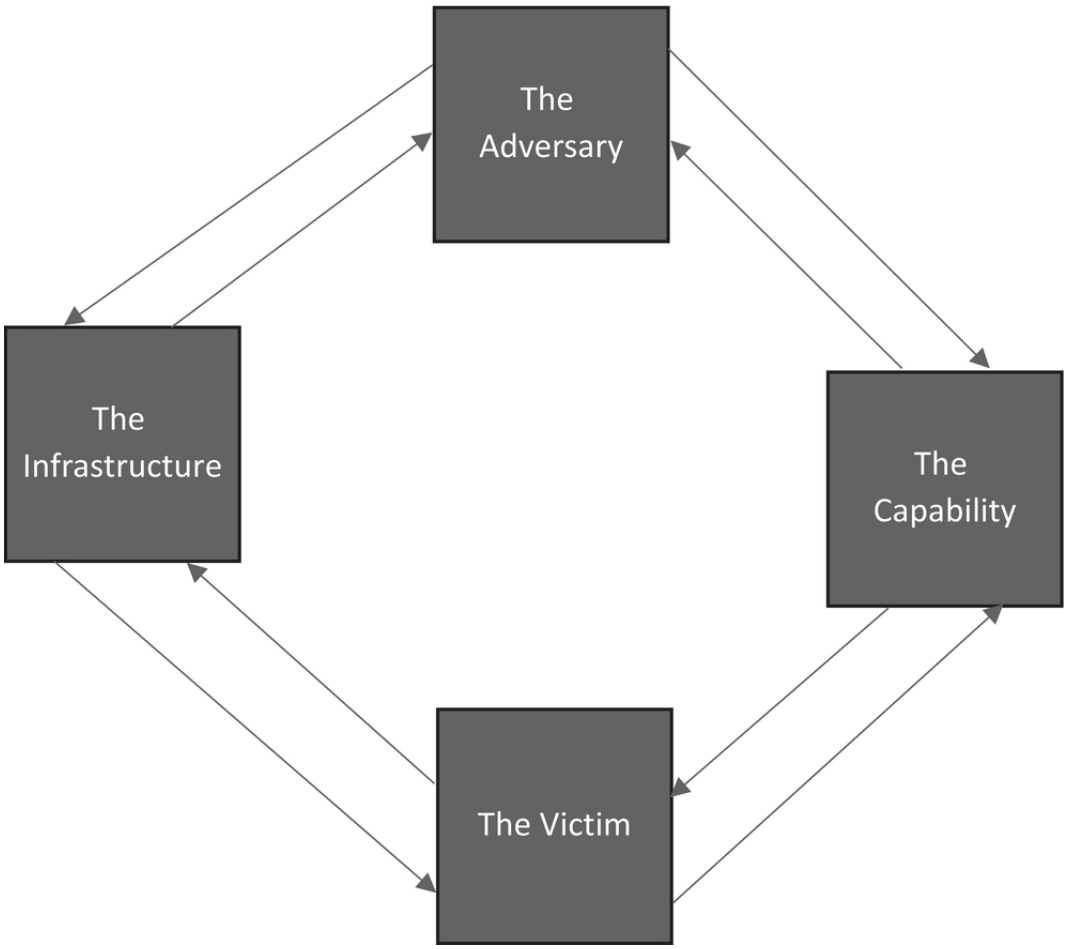


Figure 1.12 An illustration of the Diamond Model of Intrusion Analysis.

The interrelationships between the components of the Diamond Model of Intrusion Analysis

There are also four of them, and they are as follows:

1. *The Adversary – Victim*:
   These are the specific interactions that take place between the Cyberattacker and the target. Questions asked here include the following:
   - Why did the Cyberattacker selected their particular target?
   - What are their motivations and objectives?
2. *The Adversary – Infrastructure*:

The Cyberattacker uses many types and kinds of technical resources. This particular relationship reflects how the attacker establishes and maintains its Cyber Attack Methodology.

3. *The Victim – Infrastructure*:
   This is the victim's direct connection to the Cyberattacker's technical resources. This particular relationship concerns the following:
   - The Cyberattacker's use of different channels and mediums
   - Their specific methods
   - The Threat Vectors that can be used against the target.
4. *The Victim – Capability*:
   This is the target's direct connection to the Cyberattacker's tools and techniques. This linkage addresses the specific tactics and Attack Signatures that the Cyberattacker uses against the target.

The meta features between the components of the Diamond Model of Intrusion Analysis

There are eight of them, and they are as follows:

1. *The Timestamp*:
   This is the actual date and time that the security breach impacted the business in question.
2. *The Phases*:
   These are the different stages in which the Threat Variant is launched and deployed.
3. *The Result*:
   This reflects how successful the Cyberattacker was in achieving their specific objectives.
4. *The Direction*:

This is the trajectory that the Cyberattacker used to get across the IT and Network Infrastructure.

5. *The Methodology*:
   This is the plan that the Cyberattacker came up with in order to launch and deploy their particular Threat Variant.
6. *The Resources*:
   These are the particular assets that the Cyberattacker used to launch and deploy their particular Threat Variant.
7. *The Technology*:
   These are the tools and devices that enabled and allowed the Cyberattacker to do what they have done in order to achieve their specific objectives.
8. *The Socio – Political*:
   This is the specific relationship that developed between the Cyberattacker and their victim. This is used mostly in modeling Social Engineering Attacks.

The advantages of the Diamond Model of Intrusion Analysis

These are as follows:

- The Indicators of Compromise (also known as the “IOCs”) can be further enriched and optimized.
- Any Pivot Opportunities that are used by the Cyberattacker can be quickly identified.
- The process can become more detailed and made more quantitative in nature by including statistical-based Hypothesis Generation and Testing.
- It is highly flexible and scalable that can lead to the development of logical courses of action to take in order to mitigate any potential

Threat Variants.

- Principles and concepts of other Cyber-related Frameworks can be easily added onto it.
- New techniques into Threat Intelligence can be potentially created.
- It can serve as a strong backbone to the CISO and their IT Security team.
- It allows for the creation detailed Intrusion Analysis.
- It can be used to identify any trends amongst the Signature Profiles of the various Threat Variants.
- It provides the ability for the CISO and their IT Security to come up with various kinds and types of Cyber Defensive Strategies.

For a scientific review of the Diamond Model of Intrusion Analysis, access the link below:

Diamond_Review.pdf

The NIST Cybersecurity Framework

This is yet another Cybersecurity Framework that was developed by the National Institute of Standards and Technology (also known as "NIST"). It was established on 12 February 2013, under Executive Order (EO) 13636 – "Improving Critical Infrastructure Cybersecurity". What separates this Framework from the others reviewed so far in this chapter is that it can be deemed to be a set of Best Practices and Standards. As a result, it consists of the following components:

1. *The Identification*:
   This is where the business needs to understand both the Physical and Digital Assets that they have, as well as the risks, and the threats that

could impact them directly. This kind of Risk Assessment typically involves identifying classifying the Critical Systems, their datasets, and their resources that need further protection.

2. *The Protection*:
   These are the controls that are needed to protect both the Physical Assets and the Digital Assets. Examples of this include the following:
   - Firewalls
   - Access Controls
   - Encryption
   - Security Awareness Training for the key stakeholders in the business.
3. *The Detection*:
   This is the ability to detect a Security Breach on a real-time basis. Ideally, the key Cyber metrics of the Mean Time to Detect (also known as the "MTTD") and the Mean Time To Respond (also known as the "MTTR") should be kept as low as possible. The controls used here include the following:
   - Intrusion Detection Systems
   - Continuous Monitoring
   - Anomaly Detection tools
4. *The Response*:
   This is how quickly the CISO and their IT Security team should respond to a security breach. Crucial documents that are needed here include the following:
   - The Incident Response Plan (which details how a Security Breach should be contained).
   - The Disaster Recovery Plan (which details how the mission critical processes of the business should be restored).

- The Business Continuity Plan (which details the long term of recovery of the business).

5. *The Recovery*:
   This is how the business will fare in the long term after they have been impacted by a Security Breach. Again, the Business Continuity Plan is of upmost importance here.

The implementation tiers of the NIST Cybersecurity Framework

There are four different ways in which this framework can be deployed, and they are as follows:

1. *The Tier 1 – Partial*:
   The deployment and implementation of Cybersecurity controls and protocols have been reactive versus proactive. The business has limited awareness of Cybersecurity Risks and severely lacks the funding and resources to enable the Information Security Policies.
2. *The Tier 2 – Risk Informed*:
   The business is more aware of what Cybersecurity Risks they potentially face. But it still lacks a planned and proactive Cybersecurity Risk Management Process.
3. *The Tier 3 – Repeatable*:
   The business has implemented a Cybersecurity Risk Management Plan. Thus, the CISO and the IT Security team can now monitor and respond effectively to the Threat Variants they face.
4. *The Tier 3 – Adaptive*:
   The business is now Cyber Resilient and continuously improves and advances the their Cybersecurity best practices and standards. As a

result, enough funding has been set aside to maintain a comprehensive Cybersecurity Risk Management Platforms at all times.

The Cybersecurity risk management platform of the NIST Cybersecurity Framework

This is also included in the NIST Cybersecurity Framework, and it includes the following:

1. *The Prioritization and Scoping*:
   This establishes the mission objectives and the Cyber Risk Tolerance of the organization.
2. *The Orientation*:
   This is a comprehensive assessment of what Physical Assets and Digital Assets the business currently has in stock.
3. *The Current Profile*:
   This is a comprehensive assessment as to how the business is currently managing their Cybersecurity Risk Posture levels.
4. *The Risk Assessment*:
   This is where the CISO and their IT Security team rank and categorize the degree of vulnerability that each Physical Asset and Digital Asset faces.
5. *The Target Profile*:
   This is where the CISO and their IT Security team create or enhance their Cyber Risk Management Goal(s).
6. *Finding Gaps and Weaknesses*:
   This is where the gaps in both the Physical Assets and the Digital Assessments are found, through the Risk Assessment that was conducted in Step #4.
7. *The Action Plan*:

In this last phase, a Plan of Action is created in order to deploy and implement the needed controls to remediate the gaps and weaknesses that were found in Step #6.

More details about the NIST Cybersecurity Framework can be accessed at this link below:

The NIST Cybersecurity Framework (CSF) 2.0

The STRIDE Threat Modelling Framework

Next in line for ascertaining the actions of the Cyberattacker is what is known as the STRIDE Model. It was developed in the late 1990s by Koren Kohnfelder and Praerit Garg, who were working at Microsoft at the time. They published this model in a technical article that was titled "The Threats to Our Products". STRIDE is actually an acronym that stands for the following:

Spoofing Identity
Tampering with Data
Repudiation
Information Disclosure
Denial of Service (DoS)
Elevation of Privilege

Each of these components are reviewed in the next subsection.

The components of the STRIDE Threat Modelling Framework

1. *Spoofing Identity*:
   This is where the Cyberattacker assumes another Identity. They most likely have heisted profile of the victim off a Social Media Platform or

even their Personal Identifiable Information (PII) datasets. They could also have used another platform that is called “OSINT”. It is an acronym that stands for “Open-Source Intelligence”. It can be technically defined as follows:

> Open-source intelligence (OSINT) is the process of gathering and analyzing publicly available information to assess threats, make decisions or answer specific questions.
>
> (What Is OSINT (Open-Source Intelligence)? | IBM)

Although this platform is used a lot for Cybersecurity, the Cyberattacker can also use it to glean more information and data of their targeted victim. Of course, there is nothing really illegal about this, since it is all publicly available.
Another way that the Cyberattacker can spoof Identity is through the use of creating a Deepfake, which was reviewed earlier in this chapter.

2. *The Tampering with Data*:
   This is where the Cyberattacker covertly steals the Personal Identifiable Information (PII) datasets of the employees, customers, and the other relevant stakeholders of the business. It can be sold on the Dark Web or even used to launch an Extortion Attack against the victim.
3. *The Repudiation*:
   This can be technically defined as follows:

> A repudiation threat involves a bad actor attacking the system without accepting their involvement in such malicious activity.
>
> (What is STRIDE Threat Model?)

A prime example of this is when the controls in the IT and Network Infrastructure cannot detect when a Cyberattacker has actually lurked into the system and has deployed a Malicious Payload that is about ready to be launched and executed.

4. *The Information Disclosure*:
   This is where the Personal Identifiable Information (PII) datasets are released to the public, whether intentionally or not. For example, this could be a Data Exfiltration Attack launched by the Cyberattacker; it could be a Data Leakage from a Cloud-based deployment either on the AWS or on Microsoft Azure, or even an Insider Attack launched by a rogue employee who has intimate knowledge of the Database Systems of the business in question.
5. *The Denial of Service*:
   This is where the server or servers are flooded with rogue data packets. The idea here is not to completely disable the server but to overwhelm its consumption and processing capabilities so that access to the shared resources that are stored on that particular comes to an almost screeching halt. These are known as Denial of Service (also known as "DoS" and Distributed Denial of Service (also known as "DDoS") Attacks. With former, only one server is targeted, but with the latter, many servers become the victim. An example of a DDoS Attack is illustrated in Figure 1.13.

Figure 1.13 An illustration of the DDoS attack. (Cyber Security Data Protection Business Technology Stock Illustration 2045900174 | Shutterstock)

6. *The Elevation of Privilege*:
   This is where the Cyberattacker goes after what are known as the "Super User"-based rights, privileges, and permissions. A prime example of this is those that are assigned to members of the IT Security team, such as those of the Network Administrator and the Database Administrator. Both of these job titles have elevated rights, permissions, and privileges in order to maintain, update, and optimize the servers that reside in their jurisdiction. An area that falls within this is what is known as Privileged Access Management, or "PAM" for short. It can be technically defined as follows.

The benefits of the STRIDE Threat Modelling Framework

This framework has a number of key benefits to it, which are as follows:

- It can be used to map out the defenses for the entire IT and Network Infrastructure of the business.

- It can be used to detect vulnerabilities, gaps, and weaknesses at a very early stage.
- It can be cost-effective, as well as scalable, effective, and efficient.
- It is a great model that is best fit for conducting Threat Hunting exercises, which was reviewed earlier in this chapter.

The PASTA Threat Modelling Framework

Another Framework that is also compatible with the others reviewed so far in this chapter is that of the PASTA Threat Modelling Framework. It is an acronym that stands for "Process for Attack Simulation and Threat Analysis". It gives a business the ability to create a well-defined process for mitigating the risks of a security breach that is launched by a Cyberattacker. What is unique about this Framework versus the others that we have examined so far in this chapter is that it views as combatting Threat Variants as a business problem. Its primary objective is to allow for the simulation of Cyberattacks that could potentially impact the applications that reside from within the IT and Network Infrastructure.

This particular Framework provides for the strategic steps that are needed to create an effective set of countermeasures in order to thwart off a Threat Variant. Furthermore, it can map potential security breaches through the various scenarios that have been created by the CISO and their IT Security team. It was created and launched in 2015 by Tony Uceda Vélez and Marco M. Morana of VerSprite Security.

The components of the PASTA Threat Modelling Framework

There are seven components to this framework, and they are as follows:

1. *The Definition of the Business Context*:

This phase examines the Cyber Risk Profile for the software application that is being developed in the very beginning stages of the Software Development Lifecycle (also known as the "SDLC").

2. *The Technology Enumeration*:
   This phase takes a closer look at the "Technology Stack" that is being used to create the software application in question.
3. *The Application Decomposition*:
   This phase examines the flow of information and data between the software application under development and the other existing software applications that currently reside in the IT and Network Infrastructure of the business.
4. *The Threat Analysis*:
   This phase examines and models the potential Threat Variants that could impact the software application that is currently under development. A prime example of this is a Web-based application. At certain points in the SDLC, the DevSecOps team will conduct various Source Code reviews to see where any potential gaps, weaknesses, and vulnerabilities could exist.
5. *The Vulnerability Identification*:
   In this phase and at certain points in the SDLC, the DevSecOps team will conduct various Source Code reviews to see where any potential gaps, weaknesses, and vulnerabilities could exist.
6. *The Attack Simulation*:
   In this phase, various Cyberattack scenarios are launched at what was discovered in Step #5. This is very often done by conducting Penetration Testing and Threat Hunting exercises.
7. *The Residual Risk Analysis*:

This is the very last phase of the Framework, and all that was discovered in both Step #5 and Step #6 are now fully remediated.

The PASTA Threat Modelling Framework is illustrated in Figure 1.14.

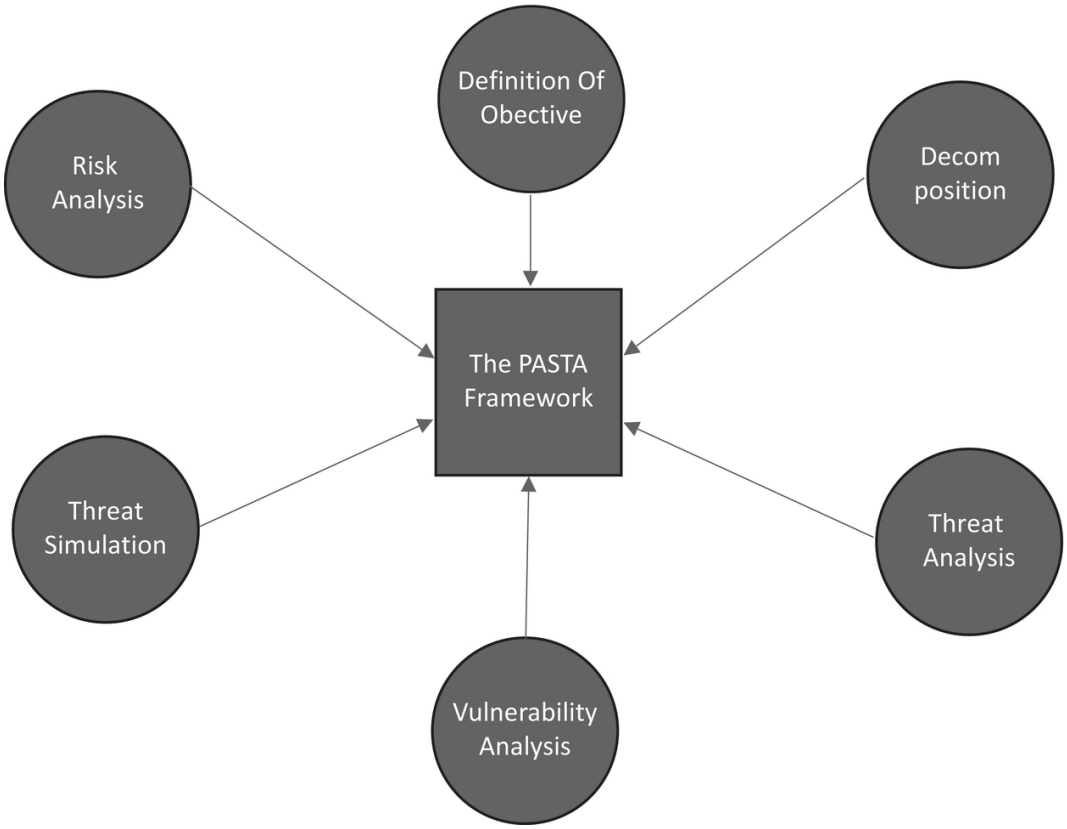


Figure 1.14 An illustration of the PASTA Threat Modelling Framework.

The characteristics of the PASTA threat modelling framework

There are numerous characteristics of this framework, which are as follows:

- It is a methodological approach, not process based.
- It is highly Cyber Risk focused, which looks at all of the quantitative variables in a Threat Variant.
- It is designed to be collaborative across all departments in a business, so that a representative sample of key stakeholders can participate in it.

- It is designed to be prescriptive in nature; in other words, its focus is on reducing the total number of gaps, vulnerabilities, and weaknesses in a software application before it is launched into the Production Environment.
- It is evidenced based, and in that, future Threat Variants are modeled only by solid information and data of what has happened in the past.
- It is meant to be a dataset compliant with the provisions and tenets of the major Data Privacy Laws of the GDPR, CCPA, HIPAA, etc.

For more details into the PASTA Threat Modelling Framework, access the link below:

PASTA_Framework.pdf

The LINDDUN Threat Modelling Framework

Another framework that is also very comparable with the others reviewed so far in this chapter is that of the LINDDUN Threat Modelling Framework. It is an acronym that stands for the following:

Linking
Identifying
Non-Repudiation
Detecting
Data Disclosure
Unawareness
Non-Compliance

This framework is further reviewed in the next subsections.

The components of the LINDDUN Threat Modelling Framework

The components of this framework are as follows:

1. *The Linking*:
   This is where all of the Personal Identifiable Information (PII) datasets are linked or combined against one another. The primary objective with this is data or actions to learn more about an individual or group; with more data on hand, more can be learned, especially about the Cyberattacker.
2. *The Identification*:
   This is where attempts are made to actually confirm the identity of an individual. It can be used typically in a Multifactor Authentication (MFA) and Zero Trust Framework approach, but it is also used to identify the Cyberattacker after they have launched a Threat Variant against the business and key pieces of evidence have been collected after a comprehensive Digital Forensics Investigation has taken place.
3. *The Non-Repudiation*:
   This is the ability to link an attribute to an individual. For example, if there is abnormal activity that has been detected from within the IT and Network Infrastructure, the log files that have been outputted by the Network Security Devices should be able to pinpoint the IP Address of the device in question, and from there, the individual that was using it.
4. *The Detecting*:
   This is the process that is used to determine the involvement of an individual based on observation. A prime example of this is when a

rogue employee is identified by yet another employee as the perpetrator of an Insider Attack.

5. *The Data Disclosure*:
   This is where the business in question goes to extreme or excessive Personal Identifiable Information (PII) dataset collection, especially when it comes to its storage, processing, sharing, and archiving for later uses. In fact, the major Data Privacy Laws of the GDPR, CCPA, HIPAA, etc. all mandate that businesses have to disclose to end users how their information and data is being used in this regard and to also give them the option to opt or, to have their Personal Identifiable Information (PII) datasets deleted from the respective Databases.
6. *The Unawareness*:
   This is actually the complete opposite of the last component. This can be viewed as the insufficient notification and/or empowerment for the end users to exercise control over their Personal Identifiable Information (PII) datasets. In fact, the Data Privacy Laws just described provide for harsh financial penalties if a business is found guilty of this, but only after an exhaustive audit has been conducted. For example, with the GDPR, the financial penalties can be 4% of the Gross Revenue.
7. *The Non Compliance*:
   This is where the business in question has not deployed and/or upgraded their new and/or existing controls in order to protect the Personal Identifiable Information (PII) datasets of their customers, employees, and other key stakeholders. Once again, the Data Privacy Laws mandate that businesses have these in place, and if not, they are then subject to an exhaustive audit and steep financial penalties.

The functionalities of the LINDDUN Threat Modelling Framework

There are three main functionalities, which are as follows:

1. *The Threat Types*:
   These are the components of the LINDDUN Threat Modelling Framework that was reviewed in detail in the last subsection.
2. *The Threat Trees*:
   These are tree-like schematic diagrams in an effort to further refine each of the seven components reviewed. The primary goal here is to provide them with more concrete characteristics, which are primarily applicability and impact.
3. *The Methods*:
   There are three main methodologies and are further reviewed in the next subsection.

The methodologies of the LINDDUN Threat Modelling Framework

There are three major methodologies for the LINDDUN Threat Modelling Framework, and they are as follows:

1. *The LINDDUN Go*:
   This is meant to be a limited approach to Threat Modelling aimed at teamwork amongst the members of the IT Security team.
2. *The LINDDUN Pro*:
   This is a quantitative approach to ascertaining Data Privacy Risks or Vulnerabilities. In order to do this, it makes use of Data Flow Diagram (also known as the “DFD”).
3. *The LINDDUN Maestro*:

This is a quantitative approach to ascertaining Data Privacy Risks or Vulnerabilities. In order to do this, it makes use of Data Flow Diagram (also known as the “DFD”) and much sophisticated Statistical Techniques.

The threat trees of the LINDDUN Threat Modelling Framework

The LINDDUN Threat Modelling Framework also makes use of what are known as “Threat Trees” or “Attack Trees”. They are technically defined as follows:

> In cybersecurity, an attack tree is a model of how a malicious actor might seek access to an IT asset, such as a system or network. Computer security professional Bruce Schneier was one of the first to develop and publicize the notion of attack trees.
>
> Attack trees have the shape of a tree diagram:
>
> - A single root node at the top represents the hacker’s ultimate goal.
> - The children of the root represent different methods that can be used to achieve this objective.
> - The children of these children represent subproblems that must be solved along the way.
>
> (What You Need to Know About Attack Trees in Cybersecurity)

In this particular framework, there are major classifications of them, and they are as follows:

1. *The Tree Basic*:

These are only the high-level aspects of the Threat Variants that are being studied and/or examined.

2. *The Tree Examples*:
   These are only the high-level aspects of the Threat Variants that are being studied and/or examined, but examples of them are also provided.
3. *The Tree All Details*:
   These are only the high-level aspects of the Threat Variants that are being studied and/or examined, but examples of them are much more detailed, such as providing information and/or data about their Signature Profiles.

An illustration of the LINDDUN Threat Modelling Framework can be seen in Figure 1.15.

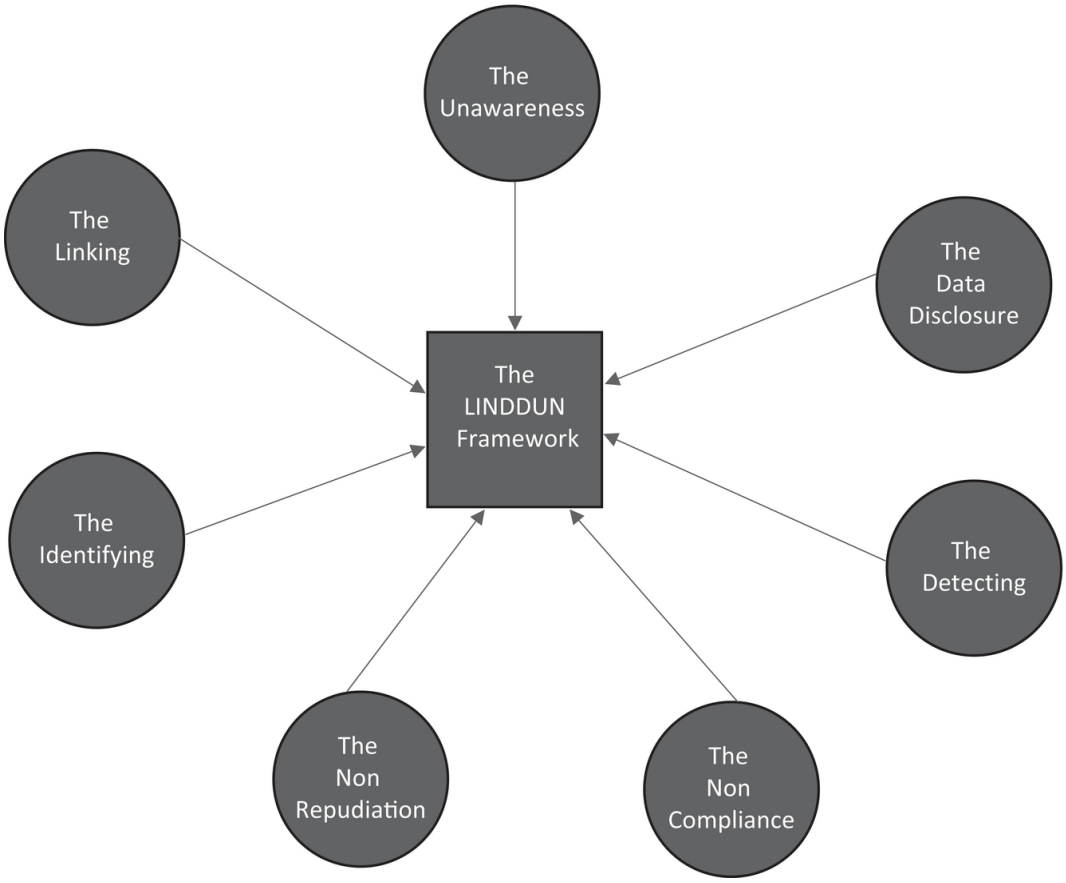


Figure 1.15 An illustration of the LINDDUN Threat Modelling Framework.

The Essential Eight Maturity Model

This is the last framework to be reviewed in this chapter. This was actually developed and created by the Australian Signals Directorate, also known as the "ASD", which is a part of the Australian Government. They have come up with something which is known as the Essential Eight Maturity Model. It was launched back in June 2017 and was published in a document known as the "Strategies to Mitigate Cyber Security Incidents". The next two subsections examine this framework in some more detail.

The components of the Essential Eight Maturity Model

There are eight of them, and they include the following:

- Patch Applications
- Patch Operating Systems
- Multi-Factor Authentication
- Restrict Administrative Privileges
- Application Control
- Restrict Microsoft Office Macros
- User Application Hardening
- Regular Backups

The first two relate to the sheer importance of maintaining a regular schedule of both downloading and deploying the needed Software Patches/Updates (and even Firmware) in order to further fortifying the IT and Network Infrastructure of the business in question.

With regards to Multifactor Authentication (also known as "MFA"), it mandates the use of differing Authentication Mechanisms that number at least three or more. For example, this could involve the use of a Challenge/Response, an RSA Token, and Biometrics (such as Fingerprint Recognition and/or Iris Recognition).

In terms of the fourth one, it highly suggests the use of using the methodology of Privileged Access Management, which was reviewed earlier in this chapter. With regards to the fifth one, it requires that all of the servers that store Web-based applications must have the appropriate controls put into place in order protect the Personal Identifiable Information (PII) datasets from a Data Exfiltration Attack.

With regards to the sixth one, it simply means employees who rely upon and create Excel-based spreadsheets need to be very careful about the use of Macros. A Macro can be technically defined as follows:

> An Excel macro is a recorded sequence of Excel commands and actions that you can play back as many times as you want. Macros can be used to automate just about any sequence of tasks in Excel.
>
> (How to use Excel macros to save time and automate your work – Computerworld)

While an Excel Macro certainly has its advantages, it can also be used to conceal instructions to a previously deployed Malicious Payload in order to launch and execute. These are very often used in Phishing Attacks.

The seventh one is also very closely correlated with the fifth one. In terms of the last and eight one, it requires a business to have a regular back-up schedule of all of the data and information that is stored in the Database Servers which reside in the IT and Network Infrastructure. It highly recommends that a business maintain at least two sets of backups, one that can be stored On Premises, and the other at some distant location, such as the Cloud (like AWS or Microsoft Azure).

The maturity levels of the Essential Eight Maturity Model

There are, at the present time, four Maturity Levels that a business can make use of in order to reach of the eight components, as reviewed in the last subsection. These Maturity Levels are as follows:

1. *The Maturity Level Zero*:
   There are grave weaknesses, vulnerabilities, and gaps in an organization's overall Cyber Security Posture.
2. *The Maturity Level One*:
   This references the Cyberattacker, and they use publicly available tools in order to create and launch their Threat Variants.

3. *The Maturity Level Two*:
   This references the Cyberattacker, and they use somewhat more sophisticated tools in order to create and launch their Threat Variants.
4. *The Maturity Level Three*:
   This references the Cyberattacker, and they use much more sophisticated tools in order to create and launch their Threat Variants, such as that of Generative AI. Also, the Cyberattacker knows how to covertly infiltrate the IT and Network Infrastructure of a business and has the ability to stay in for very long periods of time without getting noticed by the IT Security team.

Finally, more details about the Essential Eight Maturity Model can be accessed at the link below:

Eight_Framework.pdf

The kinds of Cyberattackers

So far in this chapter, we have covered the following:

- Some of the major Cyber Threat Variants.
- A chronological overview into the evolution of Cybersecurity.
- The tools that are available to detect and mitigate the Cyber Threat Variants, which include the following:
  - Penetration Testing
  - Vulnerability Scanning
  - Threat Hunting
- The various frameworks for Threat Variant Modelling include the following:
  - The MITRE ATT&CK Framework

- The Lockheed Martin Cyber Kill Model
- The STRIDE Threat Modelling Framework
- The PASTA Threat Modelling Framework
- The LINDDUN Threat Modelling Framework
- The Essential Eight Maturity Model

There is a common myth that a Cyberattacker is just a "Cyberattacker". However, this is far from the truth. There are different "brands" of them, and they are reviewed further in this section of this chapter.

Here are the major classifications of them:

1. *The Career Cybercriminal*:
   This kind of Cyberattacker's main intention is to steal Personal Identifiable Information (PII) datasets data for their own financial gain. They can work alone or in a group, but their driving goal is huge financial gain. It is important that is not just PII datasets that are the prime target, it can also include credit card numbers, bank account information, etc.
2. *The Hacktivist*:
   This kind of Cyberattacker much more driven by political, social, or ideological causes. Interestingly enough, financial gain is not their primary motivation. Prime targets here include organizations, non-profit businesses, etc.
3. *The State Sponsored Actor*:
   These are Cyberattackers from various government-backed entities. Their primary goal is to engage in Cyber Espionage, Sabotage, or other offensive activities to advance the interests for their nation. Examples of these kinds of nations include China, Russia, North Korea, and Iran.
4. *The Insiders*:

These are typically rogue employees of a business whom have intimate knowledge of the IT and Network Infrastructure of the business. Insider Attacks are often very difficult to detect, until it is literally too late. Actually, there are three distinct types of Inside Attackers, and they are as follows:

- *Malicious Based*:
  These are legitimate attempts that are made by an Insider Attacker in order to gain access to and potentially inflict grave damage upon the IT and Network Infrastructure of the business.
- *Accidental Based*:
  These are mistakes that are accidentally done by an employee. The most common example here is when they accidentally delete an important file.
- *Negligent Based*:
  These are when employees purposely avoid the Security Policies of the business. A prime example of this is: the business has strict policies for external file sharing. But in order to combat this, the employee could very well use an application that is available on the Public Cloud applications so that they can work at home. Another good example is what is known as “IT Shadow Management”. It can be technically defined as follows:

> Shadow IT is the unauthorized use of any digital service or device that is not formally approved and supported by the IT department.
>
> (What is Shadow IT? Defining Risks & Benefits | CrowdStrike)

This is a phenomenon that is based more out of the sake of convenience for the employee and the reluctance to change to a new application. For example, the IT Security could mandate the use of a newer file backup system, but because the employee is resistant to change, they could secretly still keep using their old system or get another package that is very similar, without getting the prior approval of the IT Security team.

5. *The Script Kiddies*:
   These are usually highly inexperienced novices who use existing hacking tools and techniques without almost no knowledge of the underlying technology. Most of these tools can be found on the Dark Web, or the novice can simply hire "as a Service" Cyberattacker in order to launch their Threat Variants.
6. *The Organized Crime Groups*:
   These are not Cyberattacking groups per se, but are rather Criminal Organizations that launch Threat Variants as part of the arsenal of broader criminal activities that include Drug Trafficking or Money Laundering.
7. *The Terrorist Groups*:
   These are Cyberattackers that form a Terrorist Organization and heavily engage in Cyberterrorist Activities in order to further cause and spread large amounts of fear.

Actual, real-world cyberattackers

The following is a listing of some live Cyberattacker Groups:

1. *The Cozy Bear*:
   This is a group based in Russia and was responsible for the 2016 hacking of the Democratic National Committee's email systems

2. *The Lazarus Group*:
   This is a North Korean-based Cyberattacker Group that launched the 2014 Sony Pictures hack.
3. *The Fancy Bear*:
   This is also a Russian Cyberattacker Gorup, which launched a Threat Variant into the World Anti-Doping Agency in 2016.
4. *The Stuxnet*:
   This was actually an ultra-sophisticated Worm that successfully targeted Iran's nuclear facilities in the late 2000s. This was led by United States- and Israeli-based Special Operations Forces.
5. *The NotPetya*:
   This was a very nefarious piece of Malware that impacted many businesses in 2017 on a global basis
6. *The Shadow Brokers*:
   This was the Cyberattacker Group that launched the WannaCry Ransomware Outbreak.
7. *The Stone Panda*:
   This is a Cyberattacker Group based in China that launched the APT10 Threat Variant. It targeted primarily Managed Service Providers (also known as "MSPs") that specialized delivering IT Services to the manufacturing industries.
8. *The Carbanak Group*:
   This was a Cyberattacker Group that targeted financial institutions worldwide and embezzled hundreds of millions of dollars through the ATM systems.
9. *The DarkOverlord*:
   This is a Cyberattacker Group that targeted primarily healthcare providers and entertainment companies, via Data Exfiltration Attacks.

10. *The Equation Group*:
    This is deemed to be one of the most sophisticated Cyberattacker Groups focusing in on Cyber Espionage, using nefarious pieces of Malware.

The types of Cyberattacks

So far in this chapter, we have covered the following:

- Some of the major Cyber Threat Variants.
- A chronological overview into the evolution of Cybersecurity.
- The tools that are available to detect and mitigate the Cyber Threat Variants, which include the following:
    - Penetration Testing
    - Vulnerability Scanning
    - Threat Hunting
- The various frameworks for Threat Variant Modelling, which include the following:
    - The MITRE ATT&CK Framework
    - The Lockheed Martin Cyber Kill Model
    - The STRIDE Threat Modelling Framework
    - The PASTA Threat Modelling Framework
    - The LINDDUN Threat Modelling Framework
    - The Essential Eight Maturity Model
- The various kinds and types of Cyberattackers.

In this section of this chapter, we now focus upon the various kinds and types of Threat Vectors that out there. It is important to keep in mind that the ones listed here are not necessarily brand new ones, but rather, they are Variations of the oldest Attack Vectors, such as Phishing.

1. *The Malware*:

   This is an acronym that stands for “Malicious Software”. It is a broad category of Threat Variants, but the common denominator amongst all of them is to harm an Endpoint or a Server, or for that matter, any sort of Digital Asset. The sampling here includes the following:

   - Ransomware
   - Trojan Horses
   - Spyware
   - Viruses
   - Worms
   - Keyloggers
   - Bots
   - Cryptojacking

2. *The DoS and DDoS*:

   These are acronyms that stand for “Denial of Service” Attack and “Distributed Denial of Service” Attack, respectively. Most of the DoS-based Attacks do not result in lost data; they are intended to bring a server literally down to its knees so that access to Shared Resources by the end user comes to an extremely slow crawl.

   While DoS Attacks originate from just one Attacking Server, DDoS Attacks are actually launched from Attacking Servers. They are much faster and harder to block than the DOS kinds of Attacks because multiple Attacking Servers must be identified in order to stop the DDoS Attack. This can even become an almost impossible task to do if the Attacking Servers are located in different countries around the world.

3. *The Phishing*:

As it has been mentioned throughout this entire chapter, Phishing is probably the oldest of all of the Threat Variants. It evolved in the early 1990s, and the first targeted victim what of AOL in the late 1990s. In this scenario, the victim is sent an illegitimate email either with a phony link or a malicious laden attachment.

4. *The Spoofing*:
   This is when a Cyberattacker masks themselves as a known or trusted source. The ultimate goal of this kind of Threat Variant is to penetrate into the IT and Network Infrastructure of a business with the end goal of stealing the Personal Identifiable Information (PII) datasets of customers, employees, and other relevant key stakeholders.
5. *The Identity Attack*:
   This kind of Threat Variant attempts to steal the entire Identity of the victim, in an effort to create fake documents such as Credit Cards and Drivers Licenses. It is even quite likely that the Cyberattacker will attempt to launch an Identity Theft Attack, which could take the victim years to recover from.
6. *The Code Injection*:
   This kind of Threat Variant happens when the Cyberattacker injects malicious lines of source code into a target computer or network to change its course of action, on an intended basis. The most common example of this is an SQL Injection Attack, where the Cyberattacker will insert malicious-based SQL Statements into the SQL Server Database.
7. *The Social Engineering*:
   Just like Phishing, this is also one of the oldest Threat Variants in existence, but it is being used much more heavily today. This is where the Cyberattacker employs psychological techniques in order to “con”

the victim into taking a desired course of action. This is always done by preying upon their vulnerable emotions, such as love, money, and fear.

8. *The Insider*:
   As it has also been examined throughout this entire chapter, this is usually when a rogue employee whom has intimate knowledge of the IT and Network Infrastructure of a business intends to cause harm to the business. These kinds of Threat Variants are often very difficult to detect, because one has to have the ability to sport abnormal behavior in a human being, which is a very subjective and risky task to accomplish. If the IT Security team is able to detect that an Insider Attack has happened, it is usually to late to do anything about it.
9. *The DNS Tunneling*:
   This kind of Threat Variant can be technically defined as follows:

   > DNS tunneling is a type of attack exploiting the Trojan horse concept where hackers embed malicious code or programs into a message that appears to be a DNS request. Since DNS is an essential component of most network and internet activity, this type of traffic is often able to pass through firewalls and other systems without much scrutiny.
   >
   > (DNS Tunneling: Step By Step Explanation)

   In other words, this is where the Cyberattacker can take a covert route to unleash malware and/or to extract data, IP or other sensitive information and/or data. This is achieved by encoding it bit by bit into what is known as a series of “DNS Responses”.
10. *The IoT*:

This is an acronym that stands for the “Internet of Things”. This is where the devices in both the physical and virtual worlds are all interconnected together. A prime example of this is the Smart Home, where kitchen appliances are connected together, and can all be activated through a voice command given to the Virtual Personal Assistant. But, while this has advantages, it has one serious Cyber Risk: With all of the interconnectivity that is taking place, the attack surface has greatly expanded that much more. So, through just one point of weakness that the Cyberattacker can easily penetrate into, a Malicious Payload can be inserted, activated, and executed to have a cascading effect on just about everything in the Smart Home.

11. *The Generative AI*:
    This was reviewed in detail at the beginning of this chapter. In this regard, probably the biggest Threat Variants are as follows:
    - Using ChatGPT to create Phishing-based emails.
    - The use of Deepfakes in order to launch Social Engineering Attacks.

Why Cyberattackers do what they do

So far in this chapter, we have covered the following:

- Some of the major Cyber Threat Variants.
- A chronological overview into the evolution of Cybersecurity.
- The tools that are available to detect and mitigate the Cyber Threat Variants, which include the following:
    - Penetration Testing
    - Vulnerability Scanning
    - Threat Hunting

- The various frameworks for Threat Variant Modelling, which include the following:
    - The MITRE ATT&CK Framework
    - The Lockheed Martin Cyber Kill Model
    - The STRIDE Threat Modelling Framework
    - The PASTA Threat Modelling Framework
    - The LINDDUN Threat Modelling Framework
    - The Essential Eight Maturity Model
- The various kinds and types of Cyberattackers.
- A review of the major Cyber Threat Variants, which include the following:
    - The Malware
    - The DoS and DDoS
    - The Phishing
    - The Spoofing
    - The Identity Attack
    - The Code Injection
    - The Social Engineering
    - The Insider
    - The DNS Tunneling
    - The IoT
    - The Generative AI

At this point, people often wonder what motivates the Cyberattacker to do what they do, which is essentially in the end, causing grave harm and damage to the victim. Although financial gain is a prime motivation, there are other reasons as well. We now review them in this section of this chapter.

So, what exactly drives the Cyberattacker? Here are some catalysts that give them motivation:

1. *Financial Awards*:
   As it was just stated, the Cyberattacker wants to hijack sensitive and/or confidential information and data, such as Credit Card Numbers, and Personal Identifiable information (PII) datasets. These can then be sold on the Dark Web, fraudulent activities, and even Extortion Attacks.
2. *The Espionage*:
   This primarily involves the Nation State Threat Actors, primarily those of Russia, Chian, Iran and Russia. The corporate sector can be involved as well, and even agencies from the United States Federal Government. The main idea here is to collect and gather Trade Secrets, and other types and kinds of Intellectual Property (also known as "IP"), in order to gain a concrete, competitive advantage over one another.
3. *The Hacktivism*:
   This is where Cyberattackers target businesses, websites, or other Federal Government Agencies to promote their ideologies and/or political causes.
4. *The Disruption*:
   In this case, the Cyberattacker is not so much interested in financial gain. Rather, what the motivation is to disrupt Critical Infrastructure, services and/or operations of any type or kind. In this instance, Critical Infrastructure includes the following:
   - Oil and Natural Gas Pipelines
   - The National Power Grid
   - Water Supply Lines
   - Food Distribution System

- Railway Systems
- Nuclear Facilities.

This will be examined in further detail in the next chapter, which is Chapter 2.

5. *The Personal*:

   This is where the Cyberattacker launches out Threat Variants in order to exact revenge and/or personal grievances, seeking revenge against a particular person, organization, or business entity.

6. *The Ransom*:

   In this instance, the primary motivation of the Cyberattacker is that of financial gain. The prime example of this is the Ransomware Attack, where the Cyberattacker deploys a Malicious Payload in order to lock up and encrypt the device and files of the victim. In turn, the Cyberattacker demands to be paid a Ransom, and in the form of a Virtual Currency, such as that of Bitcoin. The reason for this is that it is much harder to track this down than the traditional forms of currency.

7. *The Competitive Advantage*:

   This is also a form of Espionage, but here the goal of the Cyberattacker is not to really cause any harm. Rather, they want to collect intelligence so that it can be used to stay ahead of their competition. This is where one Cyberattacker tries to show their prowess over other Cyberattackers with extra knowledge that they have just gained.

8. *The Thrill*:

   This is where the Cyberattacker is primarily motivated by the allure of the fame and glory that is associated with hacking into an IT and Network Infrastructure of a business. In other words, all they simply want to have are “bragging rights”.

The capabilities of the Cyberattacker

As we have seen throughout this entire chapter, the common denominator of the Cyberattacker is their uncanny ability to create new Threat Variants and launch/execute them onto their victim. But the question that often gets asked is this: “What are their specific capabilities?” Here is a sampling of some them:

- The creation, development, and deployment of all types and kinds of Malware.
- Exploitation of gaps, weaknesses, and vulnerabilities in all kinds of types of systems.
- The creation and launching of both Phishing and Social Engineering Attacks.
- The launch of Identity Theft, which also includes Credit Card Theft.
- Engaging in Money Laundering Activities.
- The defacement of websites and their corresponding servers through the launch of Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks, and/or other means as well.
- Launching Data Breaches, with the most common of these being the Data Exfiltration Attacks to both On Premises and Cloud-based IT and Network Infrastructures.
- The sheer manipulation of the major Social Media Platforms.
- The launching of very targeted Security Breaches.

The major Cyberattacks that have transpired

In this last section of this chapter, we take a deeper dive into some of the major Cyberattacks that have occurred in the last few years.

The major Cyberattacks in 2024

1. *The Loan Depot Ransomware*:
   In January of last year, the LoanDepot, which is a major mortgage lender, was hit by a large scale Ransomware Attack that impacted almost 17.0 million customers.
   This included the following:
   - Social Security Numbers
   - Bank Account Numbers
   - Email addresses and other physical street addresses.

   In the end, the LoanDepot incurred costs of over $27 million.
2. *The Schneider Electric Ransomware*:
   In the same time frame, the Cyberattacking Group known as “Cactus” penetrated into the IT and Network Infrastructure of Schneider Electric. In the end, there was over 1.5 terabytes of data that was heisted. The following customers of Schneider Electric were impacted:
   - Allegiant Travel Company
   - Clorox
   - DHL
   - DuPont
   - Hilton
   - Lexmark
   - PepsiCo
   - Walmart
3. *The Kawasaki Motors Europe Breach*:
   This company was the victim of a major security breach which caused them to take the entire IT and Network Infrastructure offline in order to contain the breach. In the end, the Cyberattackers stole 487 GB of data, which included the following:

- Business Documents
- Financial Information and Data
- Banking Statements
- Dealership Information and Data
- Internal Communications Documents

4. *The Crowdstrike Incident*:
   In July of last year, CrowdStrike caused significant disruptions and downtimes across many industries on a global basis. The culprit of this was a flawed update to a software security module of CrowdStrike that affected well over 8 million Microsoft Windows devices. There were other disruptions as well, which included the following:
   - Airlines
   - Major Financial Institutions
   - Healthcare Providers
   - ATM Machines all over the world.

   The total cost of this impact was well over $1 billion.
5. *The Salt Typhoon Breach*:
   This was launched by a Nation State Actor, which was China. It impacted at least eight major United States Telecommunications companies, and the following items were exfiltrated:
   - Voice Information and Data
   - Video Information and Data
   - Text-based Communications that originated from the DoD

The major Cyberattacks in 2023

1. *The ICBC Financial Ransomware Breach*:
   This actually occurred in November of 2023. This was an actual Ransomware Attack that also impacted the IT and Network

Infrastructure of the United States Treasury. As a result, this brokerage firm could not settle that led to a loss of over $9 billion.

2. *The MGM Social Engineering Attack*:
   In September of 2023, the MGM Resorts International entity fell victim to a Social Engineering Attack which is known as "Vishing". It can be technically defined as follows:

   > Vishing, short for voice phishing, refers to fraudulent phone calls or voice messages designed to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details. These details can then be exploited for criminal activities such as fraud, identity theft, or financial theft.
   >
   > (What Is Vishing? – Cisco)

   This was launched when the Cyberattacker found the victim's information and data on LinkedIn, and because of that, they were able to impersonate the victim and place a Vishing call to the IT Security team at MGM. Because of this, there able to gain the Privileged Access Credentials to the entire IT and Network Infrastructure. In the end, this caused MGM overall $10 million in damages.
3. *The Boeing Ransomware Attack*:
   This happened in October 2023. Like the Crowdstrike incident, this was caused by an unknown vulnerability in its Citrix's software, which was known as "Citrix Bleed". In the end, more than 43 gigabytes of information and data were stolen.
4. *The British Library Ransomware Attack*:
   This was a massive Ransomware Attack against the United Kingdom's largest Library System. In the end, it cost the entity well over 7 million Pounds, which translates to $869,457,211.00 IN today's currency.

5. *The True Pill Attack*:

   This happened in August of 2023. The cause of the Cyberattack to this day still remains unknown, but it affected over 2.3 million patients, in a massive data heist which included the following:

   - The contact information of the patient
   - All of the medications that they were taking
   - The names of the Primary Care Physician

6. *The 23 and Me Breach*:

   This happened in October 2023. Over 14,000 Personal Identifiable Information (PII) datasets were stolen, which impacted almost 7 million end users.

7. *The Mister Cooper Ransomware Attack*:

   This was a Ransomware Attack, that impacted over 14 million individuals and cost the company well over $25 million, making it one of the costliest Ransomware Attacks to have happened.

8. *The Dollar Tree Third-Party Breach*:

   This happened in August 2023. What makes this different from the other Cyberattacks reviewed so far is that it involved a Third-Party Supplier, known as Zeroed-in Technologies, LLC. They were impacted by a security breach which in turn affected the Dollar Tree, in which the Personal Identifiable Information (PII) datasets were stolen, and this also included Social Security Numbers of both customers and employees. In the end, over 2 million end users were impacted.

9. *The DP World Australia Breach*:

   This happened in November of 2003. This entity handles well over 40% of Australia's total number of imports and exports. The Cyberattack caused the backup of more than 30,000 shipping containers not being delivered on time.

10. *The Ardent Health Services Ransomware Attack*:
    This happened in November of 2023. This was a Ransomware Attack, and it impacted over 30 critical care units in a wide range of hospitals. Because of this, many needed medical procedures could not be done for the patients on time, when they needed it.

In the next chapter of this book, we provide an overview into Supply Chain Attacks and probably the most vulnerable systems, which are the Critical Infrastructure.

Chapter 2

An overview of Supply Chain Attacks and Critical Infrastructure

DOI: 10.1201/9781003585916-2

So far in this book, our last chapter reviewed the following as it relates to the Cyberattacker.

So far in the last chapter, we have covered the following:

- Some of the major Cyber Threat Variants.
- A chronological overview into the evolution of Cybersecurity.
- The tools that area available to detect and mitigate the Cyber Threat Variants, which include the following:
    - Penetration Testing
    - Vulnerability Scanning
    - Threat Hunting
- The various frameworks for Threat Variant Modelling include the following:
    - The MITRE ATT&CK Framework
    - The Lockheed Martin Cyber Kill Model
    - The STRIDE Threat Modelling Framework
    - The PASTA Threat Modelling Framework
    - The LINDDUN Threat Modelling Framework
    - The Essential Eight Maturity Model
- The various kinds and types of Cyberattackers.

- A review of the major Cyber Threat Variants, which include the following:
    - The Malware
    - The DoS and DDoS
    - The Phishing
    - The Spoofing
    - The Identity Attack
    - The Code Injection
    - The Social Engineering
    - The Insider
    - The DNS Tunneling
    - The IoT
    - The Generative AI
- Why Cyberattackers Do What They Do
    - The Capabilities of the Cyberattacker
- The Major Cyberattacks That Have Transpired

In the last section of the last chapter, there was an extensive review done of the major Cyberattacks that have transpired in both 2023 and 2024. While most of them were the Ransomware Attacks or Data Exfiltration Attacks, a couple of them had to do with what are known as Supply Chain Attacks. In this regard, it was the one from Crowdstrike that is the most similar to this kind of Threat Variant.

When one thinks of a Supply Cain Attack, the thoughts of a security breach impacting the logistics and distribution often come to mind, such as that of UPS or FedEx. While to a certain degree this is true, when it comes to Cybersecurity, the meaning of a Supply Chain Attack carries a completely different connotation. For the purposes of this book, it can be technically defined as follows:

> A supply chain attack is a type of cyberattack that targets a trusted third-party vendor who offers services or software vital to the supply chain.
>
> Software supply chain attacks inject malicious code into an application in order to infect all users of an app, while hardware supply chain attacks compromise physical components for the same purpose.
>
> (What Is a Supply Chain Attack? | CrowdStrike)

In other words, a Supply Chain Attack is actually launched from a third-party supplier that the business has hired. This might be a for a number of reasons, but the most common one is for them to take over some of the mission critical processes and operations from the business. In the case of Crowdstrike, although a third-party supplier was not used, the effects were the same. So in a theoretical sense, the third-party supplier or the vendor themselves has one point of vulnerability that the Cyberattacker can easily penetrate into.

Once they are in, they can then deploy a Malicious Payload, and then later they can be launched and executed at the whim of the Cyberattacker. Once this has happened, this will then trigger a cascading effect that can literally hijack thousands of devices all at once on a global basis. This can happen in just a matter of minutes. In the case of Crowdstrike, a rogue piece of content somehow managed to get its way into the one application that most of its customers utilize. In just a short period of time, hundreds of thousands of people and businesses were impacted.

This is illustrated in Figure 2.1.

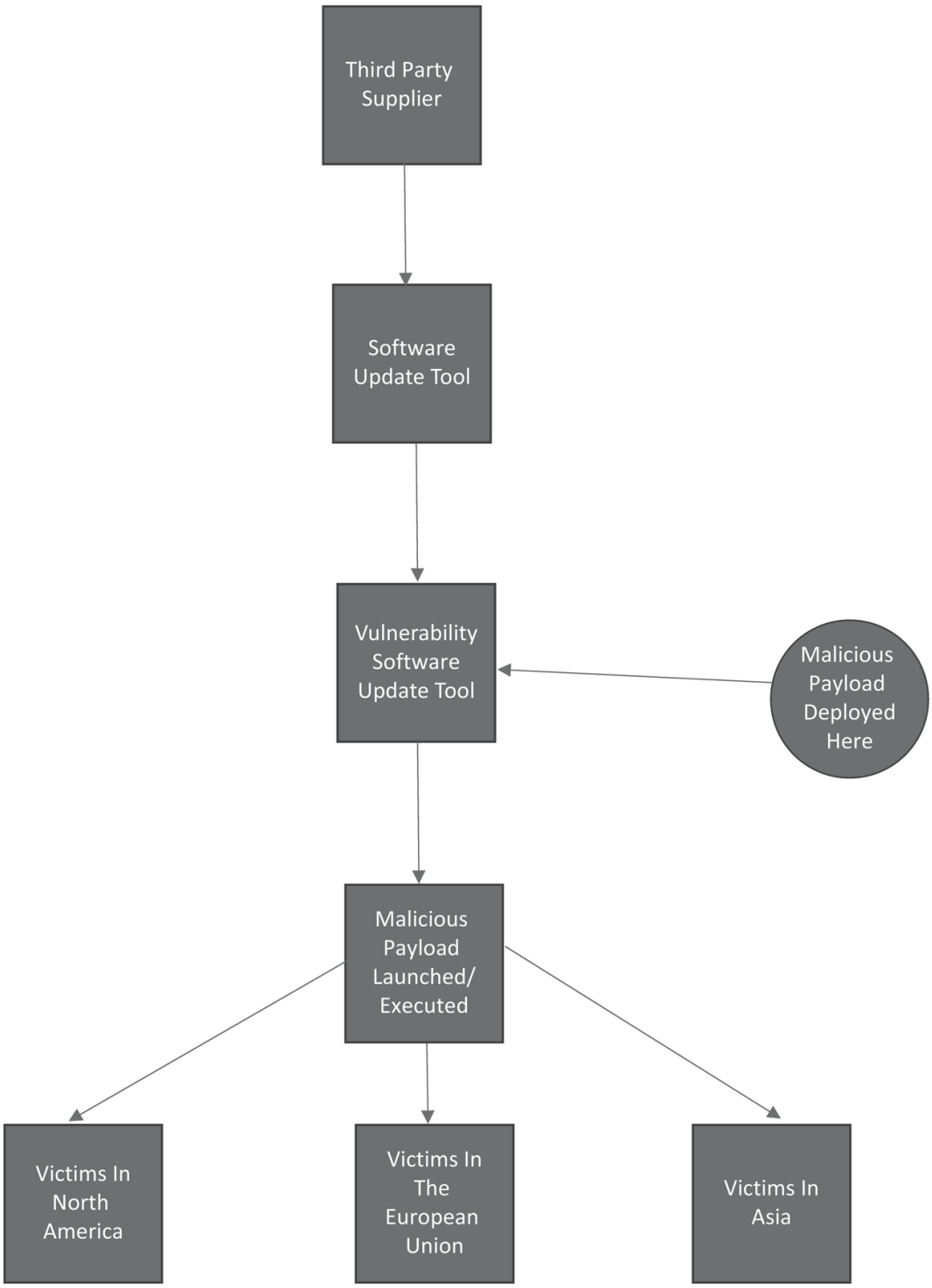


Figure 2.1 An example of a Supply Chain Attack.

Here is a breakdown of the above illustration:

1. The third-party supplier has a software upgrade tool. Rather than having each end user manually download all of the needed software patches and updates, this tool can be used to deploy them to everybody at all once.
2. However, there is a vulnerability in this tool that the Cyberattacker can easily manipulate and insert a Malicious Payload into. In this scenario, the IT Security team does not even know about it. This also becomes what is known as a Zero Day Attack, and it can be technically defined as follows:

> A zero-day exploit is a cyberattack vector that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. "Zero day" refers to the fact that the software or device vendor has zero days to fix the flaw because malicious actors can already use it to access vulnerable systems.
>
> (What is a Zero-Day Exploit? | IBM)

3. The Malicious Payload is then launched and executed.
4. Then, the victims, on a global level, are then impacted all at once, in just a matter of minutes.

Given the breadth and scope of the Supply Chain Attack, many Cyberattackers are now opting to use this kind of Threat Variant, primarily because through just one point of entry, a lot of damage can be done in just a very short period of time. In fact, this venue would be "prime time" in order to launch a massive Ransomware Attack.

In this regard, trying to vet a third-party supplier and managing the risk that is associated needs to be addressed and is now covered in the following

sections.

The types of third-party risks

At the present time, when one hears the term “risk”, the thoughts of Cybersecurity threats from your third party transmitted down to your business very often come to mind. But keep in mind, there are other types of third-party risks that can be just as lethal to your business. Some of these include the following:

1. *Brand Risk*:
   This is also commonly referred to as “Reputational Risk”. This occurs when your third party has received any sort of negative attention, in news headlines or other forms of media outlets.
2. *Process (Operational) Risk*:
   This happens when a mission critical process breaks down for a period of time at the location of your third party. This can greatly impact your supply chain and put a serious cringe on product/service delivery to your customers.
3. *Disaster Recovery Risk*:
   In the advent that your third-party experiences a massive Cyberattack or other type of natural disaster, this could also have a severe impact on your own business as well. Thus, it is important that they not only have a solid Disaster Recovery (DR) plan in place, but a Business Continuity (BC) plan as well in order to prove their level of “Cyber Resiliency” to you (this merely refers to how quickly they can bounce back from a security breach).
4. *Data Privacy Risk*:

This is probably one of the biggest areas of concern at the present time. For example, there are good chances that you will be sharing confidential information (especially as it relates to your customers) with your third party. Just as much as you are vigilant in protecting, you have to make sure of this with them as well. If there are any security breaches that occur with your third party which involves the loss or malicious heisting of information/data, you will be held responsible, not them. This issue has become much more prevalent with the recent passages of the CCPA and the GDPR.

5. *Noncompliance Risk*:
   Just as much as you have to be compliant with the recent regulatory frameworks, so does the third party that you onboard. If they are not, there are good chances that they could be audited, and your business could also be dragged into it as well.
6. *Credit (Financial) Risk*:
   This kind of risk can also be of grave concern, especially during this time of lockdowns. If your third party does not have enough cash flow or reserves on hand to sustain themselves during this pandemic, you should act quickly in order to find another suitable that can deliver you need right on time, without any disruptions to your own processes.
7. *Geopolitical Risk*:
   This typically happens when your third party is located in an entirely different country. For instance, various political events could rock your supply chain, or even Insider Attacks can damage the parts that you need in order to produce and deliver a quality product.

How to manage third-party risks

There are numerous steps that you can take to mitigate your level of risk to the third parties that you hire, which include the following:

- *Hire a Dedicated Individual*:
  Being a member of the C-Suite or even the business owner, your time is obviously at a premium. Therefore, you should hire somebody whose sole job is to locate and vet out possible third-party vendors as your company needs them. Probably one of the biggest qualifications that you should require of he or she is their ability to take a close look at the security policies and the respective level of enforcement at the third party you are looking at hiring. Also, they should be able to carefully examine just how well they protect their own confidential information/data, as this will be a reflection as to how they will treat the ones that belong to your organization.
- *Launch a Very Detailed Due Diligence Process*:
  By this, you are literally conducting a background check on the third party you are planning to hire. For example, not only should you examine their financial stability and brand reputation, but you also need to pay very careful attention as it relates to Cybersecurity. For example, you need to make sure that their practices and policies mesh up to the high standards that you have set forth for your own company. Not only this, but to a certain degree, your dedicated third-party manager should be allowed to examine just how well fortified the lines of defenses are fortified at your potential third party, as it relates to their IT and network infrastructures. Keep in mind that any security breach that impacts them could also hit you as well, as the Cyberattacker will be on the lookout for these kinds of business relationships.
- *Create an Iron Clad Contract*:

Before you actually hire a third party, you must have a contract in place that spells out in detail the responsibilities that the third party has to you, and this has to be enforceable at any time. For instance, if you suspect that there could be a lack of enforcement as it relates to internal controls, then you should have the right to inspect that and recommend a corrective course of action that should be implemented ASAP. Also, the contract should stipulate that you can conduct an audit any time that is deemed necessary in order to make sure that your third party is living up to its end of the obligations.

How to vet out a third-party supplier

1. *Hit Upon the Key Components*:
   When you are vetting out a potential, third party with whom you are interested in working with, there is the strong temptation to give them the proverbial 3rd degree. But stay away from that. There will be a time and place when you will be doing a deeper dive into the way they conduct business, especially from the standpoint of Cybersecurity. But first, as the title of this subsection implies, focus upon the important things first. This means getting to know the people at this third party with whom you will be potentially dealing with and understand how they do business with others. But most importantly, engage conversations with those people who will be handling and processing your confidential data, especially when it comes the Personal Identifiable Information (PII) datasets. You need to feel comfortable working with them, and they need to feel likewise with you. Once you have some sort of connections established, then you can do that deeper dive into how they conduct their Cyber practices, and more

importantly, what steps they will take to help safeguard your information and data that you will be entrusting them with.

2. *You Are Not Alone in This Process*:
   Very often, business owners, especially the SMB ones, tend to feel uncomfortable at first when trying to interview those external, third parties that they want to work with. This is perfectly understandable, and keep in mind, you can get help with this. For example, as you engage with conversations, you can have your attorney present or even have other members of your IT Security team present with you as well. Or you can even create a special advisory board and they can be present as well. In hindsight, this is probably the better approach to take, as two (or more heads) are better than one in order to gauge how a potential relationship could possibly work.
3. *Get a Holistic Picture of What Their Infrastructure Looks Like*:
   To be honest, the word of Cybersecurity has become extremely complex, and in fact, a very difficult one to deal with. This is not only triggered by the threat variants that are bombarding businesses on a daily basis, but also now one has to deal with all of the nuances of the data privacy laws such as that of the GDPR and the CCPA. If you are not compliant, you could face some very serious audits and penalties in the process. But to make matters even worst, if you hire an external third party and *if they are hit by a security breach that has impacted your PII datasets, you will be held responsible, not them*. So in this regard, once your connections have been solidified enough, you will need to do that deeper dive into what their IT and Network Infrastructures look like. But yet once again, you need to take a soft and gentle approach into this as well. After all, *you will now be probing into them, and there could be reservations even here as well*.

So what are some of the steps that you can take? Well, one approach would is to use the survey, or questionnaire approach. Obviously, coming up with something like this from scratch is an extremely difficult task, but there are options out there. For example, you have what is known as the Cloud Control Matrix, aka CCG. This a template that you can use to judge just how secure the Cloud-based environment is of your potential, third-party vendor, especially if you they are going to store your stuff in there. The link to this is:

https://cloudsecurityalliance.org/research/cloud-controls-matrix/

The other is the Standard Information Gathering template, aka SIG. This template is broken down into different questionnaire sections which include the following:

- Data storage and encryption
- IAM
- Cyber controls
- Procedures for Incident Response/Disaster Recovery/Business Continuity.

  The link for this is:

  https://sharedassessments.org/sig/

The Critical Infrastructure

As its name suggests, this is a huge component of the United States Economy, and the sustainability of the overall economy. When one thinks of this, the thoughts of huge buildings, and the Supply/Logistics Chains very often come to mind. While this is true to a certain extent, Critical Infrastructures are those areas that provide and support some of the most basic needs American Citizens in order to live on a daily basis. In this manner, Critical Infrastructure can be technically defined as follows:

> Critical Infrastructure are those assets, systems, and networks that provide functions necessary for our way of life. There are 16 critical infrastructure sectors that are part of a complex, interconnected ecosystem and any threat to these sectors could have potentially debilitating national security, economic, and public health or safety consequences.
>
> (Critical Infrastructure Security and Resilience | Cybersecurity and Infrastructure Security Agency CISA)

These sixteen different pieces of Critical Infrastructure are as follows:

- The Chemical Sector
- The Commercial Facilities Sector
- The Communications Sector
- The Critical Manufacturing Sector
- The Dams Sector
- The Defense Industrial Base
- The Emergency Services Sector
- The Energy Sector
- The Financial Services Sector
- The Food Distribution System
- The Federal, State, and Local Government Agencies
- The Healthcare Sector
- The Transportation Systems Sector
- The Water/Waste Water Treatment Sectors

As just mentioned, while the above serve as a primary backbone to the overall well being and functioning of the United States, it is very important to keep in mind that the technologies that these pieces of Critical

Infrastructure are extremely outdated, for the most part. Many of these are now legacy-based systems, having been created and deployed in the 1960s and the 1970s. In fact, many of the vendors who supplied the parts for the construction of these legacy-based systems are now longer even in existence.

Because of this, there is now a huge problem, from the standpoint of Cybersecurity. Since there are no quick available parts for these pieces of Critical Infrastructure, one simply cannot rip out these legacy systems and attempt to put new ones into place. If this were happened, the new parts would have to be made from scratch, which would cause an enormous level of downtime, which would be detrimental to the United States economy. But they have to be updated the latest Cybersecurity tools, in order to fend off any Cyberattacker in launching a Threat Variant against them.

But these legacy systems that make up these pieces of Critical Infrastructure have to able to interoperate with these new Cybersecurity features. This in lies the second problem as well. It can take a very long time in order to for this happen. Thus, given these huge vulnerabilities, gaps, and weaknesses that exist in these Critical Infrastructures and the long lag time, this serves as two very prime opportunities for the Cyberattacker to penetrate into and deploy some very nefarious pieces of Malicious Payload.

We now review all of this in the next sections of this chapter.

Introduction – what is SCADA?

A Supervisory Control and Data Acquisition (SCADA) system is an automated control system which is used primarily in Critical Infrastructure. This includes areas such as follows:

- Energy
- Gas and Oil
- Water
- The Electricity Grid
- Nuclear Facilities
- Power Plants
- Food and Agricultural Processors.

Because of the gravity of these applications, a SCADA System will be on the target list for the Cyberattacker. For example, multiple cities across the United States can be impacted, with multiple outages occurring at gas stations, electrical power plants, water supply lines, etc. In other words, our lives will come to a complete halt.

The security issues of SCADA

There are key security issues with SCADA, and the major ones are as follows:

- *Outdated Technologies*:
  Many of the SCADA Systems that are in use today have been deployed several years ago. Back then, Cybersecurity was barely an issue, so more consideration was given to physical security controls. The major concern now is that the SCADA system will be used as a point of entry to launch an attack on a Critical Infrastructure.
- *Open Visibility*:
  Because SCADA Systems were deployed so long ago, the actual physical layout as to where they would reside within a business was not taken into consideration. As a result of this, many systems are in open, and because of that, there are greater chances of an Insider

Attack. There is a growing awareness in this aspect, and businesses that make use of SCADA are trying to put advanced physical controls in place to protect it. But the main problem is that these newer technologies have to be added onto the existing legacy security system which is in place. There can be interoperability issues with this, thus creating more gaps and weaknesses in an already fragile environment.

- *Network Integration*:
  SCADA Systems were designed to operate by themselves, meaning any future integration into other technologies was not even considered. With the advent of the Internet of Things (IoT), everything is now interconnected with each other, even the SCADA systems. Once again, there are interoperability issues that are coming out, and this increased interlinking is also expanding the attack surface for the Cyberattacker.

In fact, just recently, one of the customers of Schneider Electric experienced a Cyberattack on their SCADA System. In this instance, the Cyberattacker(s) took complete advantage of a vulnerability within the firmware that was used, and from there was able to launch a zero-day privilege escalation attack. This allowed them to gain control of the entire emergency shutdown process.

Other attacks on SCADA Systems include the following:

- In March 2018, a Cyberattack disrupted the power lines that fed into the natural gas pipelines all across the United States.
- In June 2016, Malware was discovered on the IT/Network Infrastructure of a major energy company based in Europe. This led to covert backdoors being created in the SCADA System with the end result being that entire European Energy Grid could have been shut down.

How to address the security issues of a SCADA System

The main issue with SCADA Systems is that a bulk of them were built in the 1970s and 1980s. Because of this and the dependency that we have upon it today, you simply cannot “rip out” the old and put in newer technology in order to secure it. Rather, you have to have to find those security tools that can be added on to the legacy architecture that is already in place.

But, in the end, it is still possible to secure SCADA Systems, and here are some ways in which it can be done:

1. Correctly ascertain all of the connections to the SCADA System. This is like conducting a Risk Assessment for an IT/Network Infrastructure.
2. Based on the above, if there are any connections that are deemed to be unnecessary, disconnect them all at once. This is like disabling service ports when they are not being used.
3. For the connections that are remaining, make sure that they are hardened to the greatest extent possible.
4. Although SCADA Systems have been built with proprietary technologies that are not designed to comingle with others, do not further implement any proprietary protocols. It is crucial at this point everything works together.
5. If possible, run a Penetration Test or even a Threat Hunting Test to see if there are any hidden backdoors in the system. Remember, the Cyberattacker of today is looking for these all the time as an easy and covert way to get entry.
6. It is important to deploy Firewalls, Network Intrusion Devices, and Routers, etc. surrounding the SCADA System so that you can be

notified in real time of any potential security breaches that may be happening. Also, make use of a 24 × 7 × 365 Incident Monitoring tool.

7. On a regular basis, conduct risk assessments and audits to all internal and remote devices that are connected to the SCADA System.
8. Like a Penetration Test, formulate a "Red Team" so that you can tear down the walls of defense to ascertain where all known and unknown vulnerabilities and gaps lie at. From there, then it is absolutely crucial that these are remedied as quickly as possible.
9. Again, just as you would for your IT/Network Infrastructure, it is important to define to roles and responsibilities as to whom will actually "protect" the SCADA System. For example, this will include those individuals that are responsible for downloading and deploying the security patches and upgrades, responding to a Cyberattack that is targeted towards it, and bringing the system back up and running after the threat vector has been mitigated.
10. Create, deploy, and strictly enforce a data backup policy, as a well as an Incident Response/ Disaster Recovery (IR/DR) Plan, and make sure that these are practiced on a routine basis. For example, data should be backed up on a daily basis (perhaps even every few hours), and the IR/DR Plan should be rehearsed on a quarterly basis.

The security risks that can potentially affect an ICS

Just like in the digital and virtual worlds, there are numerous threats that can affect the ICS of any type or kind of Critical Infrastructure. Some of these are as follows:

1. *Air Gapping Will No Longer Work*:

As it was reviewed earlier, many pieces that make up a Critical Infrastructure were built in the late 1970s to early 1980s. Because of how long they have remained in place, one cannot just rip out these old pieces and put in new ones back in place. Back then of course, the threats of Cyberattacks was not even a concern. The main point of contention was that Physical Access Entry. For example, what if an impostor was able to gain entry, and misconfigure any settings? Or what if there was a rogue employee intent on launching an Insider Attack? One of the biggest security measures that could be afforded during those times is what is known as "Air Gapping". In a way, this is very similar to dividing up your IT/Network Infrastructure into different regimes, also known as "Subnets". With Air Gapping, the ICS network was completely isolated from the rest of the Critical Infrastructure. The theory was that if an Insider Attack were launched, any effects from it would not be transmitted down to the ICS System. But even now, Air Gapping is not a feasible solution to protect against Cyberattacks. The primary reason for this is that both the physical and digital/virtual worlds are now coming together and being joined as one whole unit through a phenomenon called the "Industrial Internet of Things" or "IIoT" for short. Because of this, trying to protect the ICS Systems is now proving to be a very difficult task, because once again, you simply cannot put in a new security system to protect it. Rather, they have to be added on as separate components, but the key is that each one of them must be interoperable with the legacy ICS network.

2. *Legacy Hardware and Software Components*:
   Because of the major difficulties in finding the right security tools to add on, many Critical Infrastructures are still using outdated hardware

and software components. Among the most at risk to a Cyberattack are the following:

- Programmable Logic Controllers (PLCs)
- Remote Terminal Units (RTUs)
- Distributed Control Systems (DCSs)

The above-mentioned devices are typically used to manage the processes as well as the sub processes of the ICS network. Because of the lack of Cyberthreats back in then, these pieces hardware and software were not built in with any sort of authentication mechanism, or even Encryption. In fact, even to this day, these components are more than likely not protected. As a result, anybody who can network access to the Critical Infrastructure could potentially move in a lateral fashion and gain access to these particular devices, and literally shut them off within minutes. The end result of this would be quite disastrous. For example, the flow of water, oil and natural gas, and even electricity could come to a grinding halt almost instantaneously, taking months to restore them back to their normal working conditions. In fact, in this situation, a Cyberattacker does not even have to be at the physical premises of the Critical Infrastructure. Since the flow of network communications is done in a clear text format from within the ICS network, a Cyberattacker could be literally on the other side of the world, and deliver their malicious payload, say, to oil refinery located in the southern United States. But worst yet, many of the Operating Systems (Oss) that are used in Critical Infrastructure are totally outdated, and even no longer supported by Microsoft. These include the likes of Windows NT and Windows XP. Also unfortunately, given the legacy structure of an ICS network, the IT departments at many Critical Infrastructures are typically far more concerned about

maintaining the stability of their IT/Network Infrastructure. They take the view that any attempt to patch the components just described will simply result in unnecessary downtime or unexpected halts to critical operations, which cannot be afforded at all costs.

3. *There Is No Clear-Cut Visibility*:
   One of the greatest advantages using a Cloud-based solution like the AWS or Microsoft Azure is that they can let you see inside your infrastructure with 100% visibility, thus letting you track down any sort of malicious activity that is taking place. But this is the total opposite with an ICS. They offer literally no visibility, thus as a result, it is almost to hard to detect if there is any suspicious behavior that is transpiring until it is way too late. Because of this, many of the settings in an ICS are difficult to configure properly in order to meet today's demand for the basic utility necessities of the everyday American.
4. *The Communications Protocols Are Outdated*:
   With the Remote Workforce today, the talk of various network protocols has now come into almost daily conversation. For example, most people have heard of TCP/IP, IPsec, 5G wireless networks, etc. For the most, the communication channels of these various protocols can operate together, in some degree or another, with virtually minimal downtime, if any. But this is not the case with an ICS network. Each one of them is outdated as well as proprietary in nature, developed decades ago. For example, this is most prevalent in the so called "Control-Layer" protocols that are used. Because of this, this is yet another backdoor for the Cyberattacker to enter into. For example, the mathematical logic that is implemented into the hardware of the ICS can be rather easily changed around, thus resulting in an unintentional flow in mission critical operations.

The top ten Cyberattacks to Critical Infrastructure

1. *Attacks on the Power Grids in the Ukraine*:
   This occurred in December 2015. The electric grid still made use of the traditional Supervisory Control and Data Acquisition (SCADA) system, which was not upgraded for the longest time. This Cyberattack impacted about 230,000 residents in that area and were without power for a few hours. Although this threat variant was short lived, it further illustrates the grave weaknesses of the Critical Infrastructure. For example, the traditional Spear Phishing Email was used to launch the threat vector, and in fact just a year later, the same of Email was used to attack an electrical substation near Kiev, causing major blackouts for a long period of time.
2. *Attack on the Water Supply Lines in New York*:
   The target this time was the Rye Brook Water Dam. Although the actual Infrastructure was small in comparison, the lasting repercussions were magnanimous. The primary reason for this is that this was one of the first instances in which in a which a nation state actor was actually blamed, and all fingers pointed towards Iran. The most surprising facet of this Cyberattack was that it occurred in 2013 but was not reported to law enforcement agencies until 2013. Even more striking is that the Malicious Threat Actors were able to gain access to the command center of these facilities by using just an ordinary dial up modem.
3. *Impacts to the ACH System*:
   Although the global financial system may not directly fit into the classical definition of a Critical Infrastructure, the impacts felt by ay

Cyberattack can be just as great. In this threat variant, it was the SWIFT Global Messaging system that was the primary target. This is used by banks and other money institutions in which to provide details about the electronic movement of money which includes ACH, Wire Transfers, etc. The Lazarus Cyberattack group, originating from North Korea, were able to gain a foothold into the banks by using hijacked SWIFT login username and password combinations. This attack has been deemed to be one of the first of its kind on the international banking sector.

4. *Damages to Nuclear Facilities*:
   Probably one of the well-known Cyberattacks on this kind of infrastructure was upon the Wolf Creek Nuclear Operating Corporation, which is located in Kansas. In this instance, Spear Phishing Emails were leveraged against key personnel working at these facilities, who had specific control and access to the controls at this Nuclear Facility. Although the extent of the damage has been kept classified, this situation demonstrates clearly just how vulnerable the United States-based Nuclear Facilities are. For example, if a Cyberattacker were to gain access into one, they could move in a lateral fashion to other Nuclear Power Plants, causing damage in a cascading style, with the same or even greater effects of that of a Thermo Nuclear War.
5. *Attack on the Water Supply*:
   The most well-known attack just happened recently in Oldsmar Florida. Although the details of this Cyberattack are still coming light, it has been suspected that the hacker was able to gain control by making use of a Remote Access tool, such as Team Viewer. But there were other grave weaknesses as in the infrastructure as well, such as a

very outdated Operating System (OS) and very poor password enforcement (such as not creating long and complex ones and rotating them out on a frequent basis). In this instance, the goal of the Cyberattacker was not just to cause damage to the Water Supply system, but to even gravely affect the health of the residents that drank the water, by poisoning it with a chemical-based lye. Luckily, an employee was able to quickly notice what was going on and immediately reversed the settings that were out into motion by the Cyberattacker. However, is it still not known yet whether this hack occurred outside United States soil, or from within. If it is the latter, then this will raise even more alarm bells that domestic-based Cyberattackers are just as much of a grave threat as the nation state actors to our Critical Infrastructure.

6. *Attack on the Healthcare System*:
   The largest health care payment platform operated by Change Healthcare was hit with a massive Ransomware Attack in February of 2024. At the time, it that handled over fourteen billion financial transactions which was launched from the Cyberattacking called the "Blackcat/ALPHV Ransomware Group". The company experienced a prolonged downtime of well over one month. This security breach became officially known as the "Triton Malware Attack".
7. *Damages to the Water Supply System*:
   A Cyberattacking Group known as the "Cyber Av3ngers" from Iran totally eradicated the automated processes of a water facility that was based in Pennsylvania, which impacted over 7,000 residents. The target was a Programmable Logic Controller (also known as a "PLC"), which regulated the water pressure at a booster pump station. A PLC can be technically defined as follows:

A Programmable Logic Controller, or PLC, is a ruggedized computer used for industrial automation. These controllers can automate a specific process, machine function, or even an entire production line.

(What is PLC? Programmable Logic Controller – Unitronics)

8. *Attack into the Power Grid*:
   In the latter part of 2022, a Cyberattacking Group known as "Sandworm" from Russia launched a security breach onto the power grid of Ukraine. This caused grave harm to the population at large, but four provinces from within the Ukraine lost electricity. The target was a vulnerable SCADA based, and the Malicious Payload was deployed as far back as 2022.
9. *Attack on the Oil Pipeline*:
   The Colonial Pipeline is one of the largest Oil Pipelines based in the United States. It was hit with a massive Ransomware Attack, and it tool over eleven days just to restore mission critical operations on a partial basis. was hit with a massive, targeted ransomware attack. The consequences of this Ransomware Attack was dire, as this specific pipeline supplied well over 45% of the fuel to the East Coast. Also, 11,000 gas stations were forced to shut down in this geographic region.
10. *Attack on Multiple Industries*:
    A Cyberattacking Group known as the "KillNet" from Russia launched a series of DDoS attacks at the allies Ukraine, that specifically targeted the healthcare systems in both the United States and the Netherlands. It also impacted the airline industry in both of these countries as well.

For a graphic visualization of these security breaches on Critical Infrastructure, access the link below:

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024

The future of Cybersecurity and Critical Infrastructure

Cyberattacks on Critical Infrastructure is occurring at a more rapid rate now, and it has garnered the attention of the industry. However, it still has not fully captured the sense of urgency yet in that something needs to be done to further fortify these structures. What is anticipated for the future? Here is a glimpse:

1. *Segmentation Could Occur*:
   In the digital world, this one of the big buzzwords that is being floated around right now. At the present time, most businesses typically have just one line of defense, that separates the threats from the external environment into the internal environment. This is very often referred to as “Perimeter Security”. But the basic flaw (and a very serious one) is that once the Cyberattacker is able to break through this, they can pretty much move in a lateral fashion and get access to anything they want to. Thus, with the implementation of MFA and the Zero Trust Framework, there have been calls now to further divide up the IT and Network Infrastructure that exists in the internal environment into smaller chunks, and this is known as “Segmentation”. Each segment would have its own set of defenses, and the statistical probability of a Cyberattacker breaking through all of these segments becomes lower each and every time, and as a result, they give up in frustration. It is hoped that this same line of thinking can also be applied to Critical Infrastructure as well, but the main problem once again, is that they all

consist of legacy computer systems, which may or may not support the Segmentation efforts. Even if they do, there is no guarantee that it will be sustainable for the long term.

2. *The Internet of Things*:
   Right now, this phenomenon has been further catapulted by the rise of the Remote Workforce, where pretty much everything has gone digital. This is the notion where all of the objects that we interact with in both virtual and physical worlds are interconnected with another. There is a great interest and even efforts are currently being undertaken to bring the world of the IoT into Critical Infrastructure. This now becomes known as the "Industrial Internet of Things" or "IIoT" for short. But it is expected that in this trend will quickly dissipate into the future, as more Cybersecurity attacks are launched against Critical Infrastructure. The reason for this is simple: With an IIoT in place, the attack surface becomes much greater, and the number of backdoors that the Cyberattacker can penetrate into is now greatly multiplied.
3. *The Financial Damage Will Escalate*:
   As more threat vectors are launched, they will obviously become more sophisticated and covert in nature. Given this, the financial toll that it will take on Critical Infrastructure that are impacted is expected to reach well over the multimillion-dollar mark. Also, is it anticipated that the downtime period to recover from future attacks will be a lot longer than what it is at the present time, thus adding more to the financial toll. Also, with the convergence that is currently taking place within the IT and the Operational Technology (OT) realms, the Cyberattacker will be able to easily gain access to either the ICS or SCADA systems via any vulnerabilities or gaps that still persist in the network of the Critical Infrastructure.

4. *A Closer Collaboration with Cybersecurity*:
   It is also expected that the leaders of Critical Infrastructure will start to work closely with the Cybersecurity Industry. Not only will there be attempts made to try to add on security tools/technologies that can interoperate with the legacy ones, but there will be even a greater effort to share threat intelligence information/date on a real-time basis so the IT Security teams of Critical Infrastructure can be much better prepared to handle any threat vectors that are looming on the horizon. This new movement has been termed appropriately the era of "Shared Responsibility".
5. *A Greater Need for Cybersecurity Insurance*:
   Essentially, by purchasing this kind of policy, a company in theory can be protected by financial losses if they are impacted by a Cyberattack. But the reality holds different in the sense that there is still a lot of confusion out there as to what will technically be covered. So while a company may think they have full coverage, the chances are still there that they will not get a 100% payout. But despite this, the Critical Infrastructure is starting to understand the need for some sort of financial protection in case they are breached. Thus, there will be a great increase in demand for Cybersecurity Insurance Policies in the coming years, in order to recoup any financial damages incurred by attacks to legacy systems.
6. *A Migration to the Cloud*:
   At the present time, there is a lot of efforts now to move On Premises solutions to a Cloud-based platform, such as that of the AWS or Microsoft Azure. While there could be some success with this as it relates to Critical Infrastructure, there is also the realization that a pure 100% migration will probably not happen. The primary reason for this

is that once again, most of the technologies that were developed for Critical Infrastructure was developed back in the 1970s and the 1980s. Thus, trying to put all of this into something as advanced as the Cloud probably will not be able to occur.

The options for Critical Infrastructure

Despite the fact that there is a huge issue between the legacy systems of the Critical Infrastructure and the Cybersecurity tools that need to be deployed onto them, in order to beef up their lines of defenses, there are still a number of options that are available. Here are some of them:

1. *The CDR*:
   This is an acronym that stands for "Content Disarm and Reconstruction". It can literally deconstruct a file into its meta data to detect and mitigate any Malicious Payloads that could exist from within it.
2. *The DLP*:
   This is an acronym that stands for "Data Loss Prevention". It can Metadata Removal, automate Document Redaction, or add a Watermark, saying "Highly Sensitive", "Highly Confidential", "Top Secret", etc.
3. *The Multiscanning*:
   With this, the Malware Detection Rates are quickened, thus alerting the IT Security team of any Threat Variants on a real-time basis.
4. *The File-Based Vulnerability*:
   This specialized tool examines for the gaps and weaknesses File-based Applications before they are deployed.
5. *The Threat Intelligence*:

This platform looks for abnormal patterns in the flow of Network Communications, which provides telltale signs to the IT Security team. There are potential Threat Variants that are looming on the horizon.

6. *The Sandbox*:
   This is a specialized kind of where the IT Security team, and even the DevSecOps team can test applications and source for any vulnerabilities, gaps, or weaknesses before anything is released into the Production Environment.
7. *The Endpoints*:
   These are the beginning and ending points of the network lines of communications from a server to a device and vice versa. To fortify these, and especially for those devices that are used in a Critical Infrastructure, Endpoint Detection and Response (also known as "EDR") is used. This can be technically defined as follows:

   > EDR is a cybersecurity technology that continuously monitors endpoints for evidence of threats and performs automatic actions to help mitigate them. Endpoints – the many physical devices connected to a network, such as mobile phones, desktops, laptops, virtual machines, and Internet of Things (IoT) technology – give malicious actors multiple points of entry for an attack on an organization. EDR solutions help security analysts detect and remediate threats on endpoints before they can spread throughout your network.
   >
   > (What Is EDR? Endpoint Detection and Response | Microsoft Security)

8. *The Endpoint Vulnerability Assessment*:

This is actually a component of the EDR solution, and it downloads and applies software updates and patches to the endpoints on an automated basis.

9. *The Malware Detection*:
   This is also a component of the EDR solution, and it looks for suspicious behavior by examining the libraries and processes that are running on the specific endpoints.
10. *The Endpoint Application Removal*:
    This too is part of the EDR Solution, and it can automatically remove software applications that are not approved by the IT Security from the employee's endpoint device.

For more details about Cybersecurity and Critical Infrastructure, access the link below:

http://cyberresources.solutions/Supply_Chain_Book/CI.pdf

The role of Operational Technology in Critical Infrastructure

It is very important to note that a critical aspect of Critical Infrastructure is what is known as "Operational Technology". It can be technically defined as follows:

> Operational technology (OT) is the use of hardware and software to monitor and control physical processes, devices, and infrastructure. Operational technology systems are found across a large range of asset-intensive sectors, performing a wide variety of tasks ranging from monitoring critical infrastructure (CI) to controlling robots on a manufacturing floor.

(What is OT Security? An Operational Technology Security? Primer)

It is also important to note that Operational Technology is also commonly referred to as just “OT”.

The components of Operational Technology

There are two of them, and they are as follows:

1. *The SCADA*:
   This is an acronym that stands for “Supervisory Control and Data Acquisition”. It was reviewed in much more detail earlier in this chapter. Their specific role in Critical Infrastructure is to collect all of the data from sensors, often at distributed sites and send it to a centralized server which then further processes this data.
2. *The IIoT*:
   This is an acronym that stands for the “Industrial Internet of Things”. It can be viewed as a subset of the Internet of Things (also known as the “IoT”) and was also reviewed earlier in this chapter. The components that make up the IIoT are as follows:
   - Generators
   - Pipelines
   - Fans
   - Programmable Logic Controllers (also known as a “PLCs”)
   - Remote Processing Units (also known as “RPUs”)
   - Industrial robots

   A PLC can be technically defined as follows:

> A programmable logic controller is a type of tiny computer that can receive data through its inputs and send operating instructions through its outputs. Fundamentally, a PLC's job is to control a system's functions using the internal logic programmed into it.
>
> (What Is a Programmable Logic Controller (PLC)? | Polycase | Polycase)

An RPU can also be technically defined as follows:

> A remote terminal unit (RTU) is a microprocessor-based electronic device used in an industrial control system (ICS) to connect hardware to a distributed control system (DCS) or supervisory control and data acquisition (SCADA) system.
>
> (What is a remote terminal unit (RTU)? | Definition from TechTarget)

The Cyber Risks of Operational Technology

As it was reviewed earlier in this chapter, the components that make up the Critical Infrastructures are made with components that are too far outdated. This was also reviewed earlier in this chapter, but it is also important to point out that there are other Cyber Risks to Critical Infrastructure as well, and they are as follows, as they relate to OT:

1. *The Lack of Visibility*:
   Many entities that are part of Critical Infrastructure don't have the right controls put into place to protect their OT Assets. Thus, it is very difficult for the IT Security team to conduct a comprehensive Risk Assessment in order to determine what the gaps, weaknesses, and vulnerabilities.

2. *The Lack of Control*:
   The IT and Network Infrastructure that make up a Critical Infrastructure are very often unsegmented. Because of this, it is very easy for a Cyberattacker to move laterally without being noticed and to spread pieces of Malicious Payloads across this entire environment. Even worse, the Communication Protocols that are used by both ICS and OT assets, are very difficult to analyze, making the detection of Threat Variants that are embedded that more difficult to detect.
3. *The Lack of Collaboration*:
   In many businesses that are involved with Critical Infrastructure, the Chief Information Security officer (also known as the "CISO") does not share much expertise or accountability for the processes and operations of the OT Assets. Thus, this leads to a fundamental lack of communications and oversight on their part.

How to counter the Cyber Risks that are associated with Operational Technology

In order to help mitigate the above Cyber Risks, deploying the following strategies is thus highly recommended:

1. *Create a Map*:
   With this, the CISO and the entire IT Security team will want to create a visualization of not just the entire IT and Network Infrastructure, but also of each and every OT Asset that is associated with it. Thus, it will be easier to conduct an efficient and effective Cyber Risk Assessment. But also, this will alleviate of the lack of communications and accountability, as it was just described in the last subsection of this chapter.
2. *The ZTF*:

This is an acronym that stands for the “Zero Trust Framework”. This was also reviewed in some detail earlier in this book. With this, the primary objective is to segment out the entire IT and Network Infrastructure into different “Zones”. Each one of them has their own layer of defenses, in which Multifactor Authentication (also known as “MFA”) is used. This is where at least three or more differing authentication mechanism in order to confirm the identity of the individual that is trying to gain access to a particular “Zone”. The logic here is that if a Cyberattacker breaks through one “Zone”, it will become statistically impossible for them to get deeper into the other “Zones” with all of the different authentication mechanisms that have been deployed. This particular methodology is also known as “Microsegmentation”.

3. *Keep an Eye*:
   With this particular strategy, the CISO and the IT Security team will want to make use of the different Cyber technologies and tools powered by Generative AI that are now available. With this, various kinds of “Heat Maps” can be created that depict the network flow of traffic that is taking place. With this, any kind or type of abnormal activity can be detected very quickly on a real-time basis.

The Cyber Frameworks for Operational Technology

In order to make sure that you (the CISO) and your IT Security team are using right methodologies for keeping with the Cyber Threat Landscape for your Operational Technology Assets, making use of at least one or perhaps even a combination of these frameworks is highly recommended:

1. *The NIST Cybersecurity Framework*:

This is a framework with a set of Cybersecurity best practices and standards recommendations developed and implemented by the National Institute of Standards and Technology (also known as "NIST"). Its framework has five key functions, which are as follows:

- Identify
- Protect
- Detect
- Respond
- Recover

To download this Framework, access the link below: http://cyberresources.solutions/Supply_Chain_Book/NIST_OT.pdf

2. *The NIST 800-82 Special Publication (SP)*:
   This is the "Guide to Operational Technology (OT) Security". It provides extensive into the Topologies, Threat Variants, and Vulnerabilities, as well as the needed controls to further safeguard your OT Digital Assets.

   To download this Special Publication (SP), access the link below: http://cyberresources.solutions/Supply_Chain_Book/NIST.SP.800-82r3.pdf
3. *The ISA99/IEC 62443*:
   These both are acronyms that stand for the International Society of Automation and the International Electrotechnical Commission, respectively. This framework provides a deep guidance into the following:
   - How to assess OT Risks.
   - How to create and implement secure components for your Digital Assets.

- The steps that are needed to create a safe and effective Industrial Network Architecture.

4. *The NERC CIP*:
   This is an acronym that stands for the "North American Electric Reliability Corporation Critical Infrastructure Protection". It is an OT framework that is specifically designed for Power Utility entities and their corresponding OT Assets. It gives detail as to how it can be made Cyber ready in an effort to thwart off an kind or type of Threat Variants.
5. *The EU NIS/NIS2 Directive*:
   This is an acronym that stands for the "Network and Information Security (NIS) Directive". It is actually a piece of legislation that mandates the implementation of OT Asset best practices, and the consequences for not doing do.

   To view this piece of legislation, access the link below:
   http://cyberresources.solutions/Supply_Chain_Book/EU_OT.pdf

An illustration of an Industrial Control System can be seen in Figure 2.2.

Figure 2.2 An example of an ICS being used. (https://www.shutterstock.com/image-photo/smart-industry-40-mangement-control-system-2525431689)

Overall, this chapter has provided an overview into what a Supply Chain Attack is and how it can impact Critical Infrastructure. A critical aspect of Critical Infrastructure in Operational Technology (also known as "OT") was also reviewed.

For a deeper dive into OT, access the link below:

http://cyberresources.solutions/Supply_Chain_Book/OT_CI.pdf

Chapter 3
Real-world Supply Chain Attacks

DOI: 10.1201/9781003585916-3

In the last chapter of this book, Chapter 4, we explored further as to what a Supply Chain Attack is all about. The following was covered:

- A formal definition of a Supply Chain Attack was provided.
- A detailed illustration was provided as to how a Supply Chain Attack can be launched.
- An overview was provided as to how Third-Party Suppliers can be a source for Supply Chain Attacks.
- A comprehensive review as to how Critical Infrastructure can be a prime target for a Supply Chain Attack.

In this chapter, we explore the concept of Supply Chain Attacks much more exclusively. We first start with some examples of real-world Supply Chain Attacks that have occurred, namely the Solar Winds security breach.

The Solar Winds Supply Chain Attack

Even though this particular incident occurred just a few years ago, this was probably the "most famous example" of what a Supply Chain Attack is and the amount of devastation that it caused. This is further reviewed in the next subsections of this chapter.

What actually happened

First, Solar Winds is a rather large software company that creates and deploys network monitoring tools. These are primarily used by larger companies in Corporate America, especially by Managed Service Providers (MSPs) that keep an eye on the IT and Network Infrastructures for their clients.

Through this, any sort or type of anomalies can be detected in the network flow of traffic, and any corrective actions can be taken immediately, which is often done remotely. One of these tools that is manufactured by Solar Winds is known as “Orion”.

It is important to note at this point that this kind of hack is different than the others that we are accustomed to hearing about. Specifically, this is known as a “Supply Chain Attack”. This simply means that rather than breaking into digital assets of Solar Winds, other third parties were targeted that made use of the Orion software package.

With this kind of approach, the Cyberattacker was thus able to breach into the lines of defense of many other private and public entities.

For example, in this situation, over 30,000 entities were impacted on a global basis. Now the question is, what was the main point of entry by which all of this havoc was created? Well, back in December 2020, many of Solar Winds’ customers that made use of Orion already had deployed two major software updates to it.

But what were thought to be system patches were actually pieces of nefarious malware, disguised to look like legitimate and safe downloads.

Even more bewildering is the fact that the Cyberattackers already had gained access to the software development platforms that created these updates going back as far as October 2019. They were able to access them through the gaps and vulnerabilities that were present in the many

Microsoft Office 365 that the employees of Solar Winds made use of on a daily basis.

So, once the Cyberattackers were in and were able to stay to that way without going unnoticed, they then examined some of the best ways in which they could cause the maximum amount of damage that was possible. They determined that inserting Trojan Horses into these platforms would be the best way to accomplish this goal.

So, in March 2020, the insertion of these malicious payloads started to take place, which would become known as “SUNBURST”. But apart from this, the Cyberattackers also created various backdoors in these payloads that would communicate with third-party servers over which they had control over.

From here, any Personal Identifiable Information (PII) datasets of both employees and customers could be covertly hijacked and either be sold on the Dark Web for a rather nice profit or be used to launch subsequent Identity Theft attacks.

But what was even worst is that these malicious payloads, backdoors, and Trojan Horses actually appeared to be legitimate modifications to the software patches and upgrades that were ultimately downloaded by the many business and government entities that made use of the Orion system.

Now, the next question is how could this level of believability actually be established, and why did it take so long to discover?

Well, the various types of malicious payloads were inserted into the “SolarWinds.Orion.Core.BusinessLayer.dll”. These are the Dynamic Link Libraries (DLLs) which were created for the software patches and upgrades exclusively for Orion. In order to get through, these DLLs were signed by Digital Certificates that verified their authenticity but were also covertly tampered with.

To make matters even worse, these DLLs were designed to be dormant for a period of 14 days so that any confidential information could be easily transmitted back to the third-party servers.

The timeline of the attack

It is important to note that the Solar Winds security breach did not happen just all at once. Rather, there was a lot of thought and planning put forth by the Cyberattackers, as the following timeline demonstrates.

From the standpoint of the Cyberattackers

September 4, 2019:
The Cyberattackers gain the first known foothold into the Solar Winds IT and Network Infrastructures.
September 12, 2019:
The Cyberattacker group deploys the first malicious payload into the Orion Software platform. This deemed to be just a test run, as the hackers used numerous servers located in various parts of the United States in order to cover their network tracks.
February 20, 2019:
The Cyberattackers do a second test run of the malicious payload in order to make sure that it will cause the damage that it was created to do.
June 4, 2019:
The test code is removed again so that it cannot be detected. After this second trial run, it appears all is working properly.

From the standpoint of Solar Winds

December 8, 2020:

Fire Eye, one of the world's leading Cybersecurity firms, made it known to the public that its IT and Network Infrastructures were hacked into and that the Cyberattackers even did away with its Red Teaming Penetration Tools.

December 11, 2020:

Fire Eye also makes the discovery that Solar Winds had also been compromised, to a great degree. The realization that this was actually a Supply Chain style attack came when Fire Eye further discovered that Orion Platform, which was used to deploy the software updates, was also hacked into between the timeframe of March 2020 and June 2020.

December 12, 2020:

Fire Eye formally notifies Solar Winds that their Orion Platform has been the vehicle for deploying the malware, through the software upgrades and patches. At this time also, the National Security Council of the United States Federal Government also intervenes in order to ascertain if any agencies had been impacted by this Cyberattack.

From the standpoint of the American public

December 13, 2020:

A number of key events occurred on this date, which are as follows:

- The Cybersecurity and Infrastructure Security Agency (aka "CISA") requires all United States Federal Government agencies to discontinue use of the Orion Platform immediately.
- Solar Winds releases temporary fixes that the impacted entities could use in order to mitigate the risk of further damage taking place.
- Fire Eye makes this Cyberattack officially a Supply Chain hack, because other third parties were also impacted, namely some of

the largest companies in the Fortune 500.
- Microsoft also intervenes and explains to the public how its customer base could be impacted by this Cyberattack.
- The hack makes the news wires for the first time, with finger pointing and blame being at nation state threat actors.

From the standpoint of risk mitigation

December 15, 2020:
Key events also transpired on this date, which include the following:

- Solar Winds releases the first software fixes to further mitigate the damage that has already been done.
- The first victims have been identified.
- The CISA and the FBI launch joint efforts into determining how the Solar Winds breach occurred in the first place and to further investigate the damage that has been done to United States Federal Government agencies.

The victims of the attack

Recent reports peg the total number at about 18,000 individual victims, which were primarily employees. Over 40 business entities were impacted, and according to Microsoft, 44% of these were technology related companies. Here is a listing of which companies were hit by this:

- United States Department of Commerce
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of State

- Department of the Treasury
- Department of Health
- Microsoft
- Intel
- Cisco
- Nvidia
- VMware
- Belkin
- FireEye
- Cisco
- Deloitte
- Mount Sinai Hospital
- Ciena
- NCR
- SAP
- Intel
- Digital Sense
- Stratus Networks
- City of Page
- Christie Clinic Telehealth
- Res Group
- City of Barrie
- TE Connectivity
- The Fisher Barton Group
- South Davis Community Hospital
- College of Law and Business, Israel
- Magnolia Independent School District
- Fidelity Communications

- Stingray
- Keyano College
- NSW Health
- City of Kingston, Ontario, Canada
- Ironform
- Digital Sense
- Signature Bank
- PQ Corporation
- BancCentral Financial Services Corporation
- Kansas City Power and Light Company
- SM Group
- CYS Group
- William Osler Health System
- W. R. Berkley Insurance Australia
- Dufferin County, Ontario, Canada
- City of Farmington
- Newton Public Schools
- Stearns Bank
- Ville de Terrebonne
- Hamilton Company
- Cosgroves
- City of Moncton
- Mediatek
- Capilano University
- City of Prince George
- Community Options for Families & Youth
- IES Communications
- Saskatoon Public Schools

- Regina Public Schools
- Public Hospitals Authority, Caribbean
- INSEAD Business School
- DenizBank
- Bisco International
- IDSolutions
- Arizona Arthritis & Rheumatology Associates
- Optimizely
- Aerion Corporation
- Pima County, Arizona
- City of Sacramento
- Clinica Sierra Vista
- Sana Biotechnology
- Ecobank
- Helix Water District
- Lukoil
- Mutual of Omaha Bank
- NeoPhotonics Corporation
- Samuel Merritt University
- College of the Siskiyous
- Vantage Data Centers
- Vocera Communications.

The lessons learned from the attack

Given the large scope of this breach, there are many key takeaways an IT Security can apply, but the following are some of the big ones:

1. *Always Know Where Your Source Code Is Coming From*:

As it was reviewed in our last article, the malicious payload was inserted into the various Dynamic Link Libraries (DDLs), and then masqueraded as a legitimate software software/upgrade to the Orion Platform. In this instance, it is unlikely that any kind of tests were conducted in the source code of the software to make sure that there was no malware in them before they were deployed onto the customer's IT/Network Infrastructure. Had this been done, it is quite probable that this kind of attack could have been stopped in its tracks, or at the very least, the damage that it created could have been contained. Therefore, it is crucial that CISOs take a proactive approach in testing all forms of source code (for example, whether it is used in creating a Web app or software patch) to remediate any gaps and vulnerabilities before they are released out to the production environment.

2. *Vetting Out of Third Parties*:

   The Solar Winds security breach has been technically referred to as a "Supply Chain Attack". This simply means that the Cyberattackers took advantage of the vulnerabilities of third parties that Solar Winds made use of in order to inflict the maximum damage possible. This underscores the importance of one of the most basic rules: Always vet your suppliers before you hire and onboard one. This means that a CISO, you need to make sure that your IT Security is carefully scrutinizing the security procedures and policies of that particular third party that you are thinking of outsourcing some of your business functions to. It must be on part of what you have in place in your organization, or even better than that. But simply making sure of what your potential supplier has put into place in terms of controls is not a one-time deal. Even after you have hired and have a business

relationship with them, you need to make sure that they are strictly enforcing these controls on a regular basis. This can take place by conducting a security audit. In the end, if your supplier becomes a victim of a Cyberattack, and the Personal Identifiable Information (PII) datasets you have entrusted the are breached, *you will be held legally and financially responsible, not them*.

3. *Keep Things Simple and Easy to Track*:
   It is simply human nature to think that investing in a large amount of security tools and technologies means that you will be immune from a security breach. But in reality, this is far from the truth. In fact, taking this proverbial "Safety In Numbers" approach simply expands the attack surface for the hacker, which was experienced in the Solar Winds breach. Instead, it is far wiser to invest in perhaps 5 firewalls versus 10 of them but making sure that they are strategically deployed to where they are needed the most. By using this kind of methodology, not only will your IT Security team be able to filter out for those threats that are real, but you will also be able to pinpoint the entry point of the Cyberattacker in a much quicker fashion, versus the time it took Solar Winds, simply due to the fact of the overload of tools and technologies they had in place. Because of this, and as it was also pointed out in the last article, it took literally months before anybody realized that something was wrong. In this regard, you may even want to make use of both Artificial Intelligence (AI) and Machine Learning (ML) tools. With this kind of automation in place, false positives will be a thing of past, and those alerts and warnings that are legitimate and for real will be triaged and escalated in a much quicker time frame.
4. *Make Use of Segmentation*:

In today's environment, many businesses are now seriously considering adopting what is known as the Zero Trust Framework. This is the kind of methodology where absolutely nobody is trusted in both the internal and external environments. Further, any individual wishing to gain access to a particular shared resource must be authenticated through at least three or more layers of authentication. But apart from this, another critical component of this the creation of what are known as "Subnets". With this, you are breaking up your entire network infrastructure into smaller ones. But what is key here is that each of these Subnets has its own layer of defense, so it becomes almost statistically impossible for a Cyberattacker to break through each and every layer. Solar Winds did not take this approach with their network infrastructure, so as a result, the Cyberattackers were able to get in through the first time around.

5. *Update Your Security Technologies*:
   With the advent of the Remote Workforce, the traditional security tools, such as the Virtual Private Network (VPN), have started to reach their breaking points, and thus their defensive capabilities. Because of this, it is important that you consider upgrading these systems to what is known as the Next Generation Firewall. These kinds of technologies are now becoming much more robust in ascertaining malicious data packets that are both entering and leaving your network infrastructure. Solar Winds did not invest properly in these kinds of upgrades, so therefore, the Cyberattackers were able to penetrate through the weaknesses of the VPNs that they were making use of.

The long-term implications

Upon a closer examination of this list of victims, one can see that this truly represents a cross section of industries. For example, public, private, educational, government agencies (on both the federal and local levels), and even nonprofit centers were heavily impacted.

It is important to keep in mind that many of these organizations listed here may not have been hit directly, but rather, they were hit indirectly because of the cascading nature of this security breach.

But none the less, this list clearly demonstrates that the Solar Winds attack has been deemed to be one of the largest in the world, and attacks like these or even worse are likely to occur and occur again until a proactive mindset is completely enforced with CISOs and IT Security teams on a worldwide basis.

The financial damage caused by the Solar Winds breach is now up to $90 Million and is estimated that it could even reach as high as $100 Billion when all is said and done.

In the end, whenever a Cyberattack hits any business entity, no matter how large or small, it is always very important to reconstruct a detailed timeline like this one. The primary advantage of this is that it can aid in the process of attribution, which is determining who the actual perpetrators are.

Also, it can pinpoint those areas in which latent evidence may lie, which is very crucial in carrying out the forensics investigation.

The Crowd Strike Supply Chain Fiasco

Early last year, the company known as Crowd Strike also succumbed to something that almost resembles the Solar Winds Supply Chain Attack, which was just examined. What separates this from the Solar Winds security breach is that is strongly purported by Crowd Strike that this was

not an actual Cyberattack, but just a gross error that occurred on their part. We examine this in more in the next subsections of this chapter.

The background into Crowd Strike

It is very important to note that CrowdStrike, that at the time before this incident actually happened, it was deemed to be one of the world's largest and most prestigious Cybersecurity Vendors that existed. It literally has clients on a global basis, and is currently based in Texas, with a workforce of well over 8,000 employees. Its revenue is well over the $3 billion mark. In fact, the following is one of their more prominent tag lines that the company has used:

> CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of risk – endpoints and cloud workloads, identity, and data – to keep customers ahead of today's adversaries and stop breaches.
>
> (https://www.computerweekly.com/feature/CrowdStrike-update-chaos-explained-What-you-need-to-know)

But apart from being of the world's leading Cybersecurity Vendors, it also plays a very distinct role in helping investigate other Cyber related security breaches as well. Examples of this include the following:

- The Sony Pictures security breach
- The WannaCry Ransomware Attack
- The 2016 security breach of the Democratic National Committee that was launched by a Cyberattacking Group from Russia

How the Crowd Strike Security Fiasco unfolded

The first signs of trouble from Crowd Strike occurred when computers, devices, and smartphones all over the world displayed the ever so infamous picture of the “Blue Screen of Death”. This comes up when a serious malfunction of the Windows Operating System (also known as the “OS”) happens. This usually indicates that a fatal error has occurred, which may or not be recoverable in the end. An illustration of this is shown in Figure 3.1.

Figure 3.1 An example of the “Blue Screen of Death”. (https://www.shutterstock.com/image-photo/merkez-july-2024-error-message-specific-2496176627)

Because of this, the IT Security teams quickly took notice of this and responded in a timely manner in the early hours of that morning. The first thought was that this was triggered by a serious glitch in Microsoft Azure, its Cloud Deployment Platform. As a result, Microsoft first launched a comprehensive investigation throughout the entire United States.

As a result of all of the detailed investigations that were carried out by Microsoft, it was later revealed that Microsoft was not to blame for this

huge fiasco, but rather it was all triggered from Crowd Strike. The culprit here was a platform from Crowd Strike that was called the “Falcon”. This is used to deploy the following services to all of its customers in one single deployment, rather than one at a time, or in separate batches:

- Next Gen Antivirus software packages
- Endpoint Detection and Response (also known as “EDR”)
- Threat Intelligence information and data
- Various types and kinds of Threat Hunting tools, and security hygiene. This is all managed and delivered through a lightweight, cloud-delivered and -managed sensor.

Once Crowd Strike took over the entire investigation, it was discovered that a faulty template which contained rogue content in the Falcon Sensor. This led to what is known as “Out of Bound Memory Failure”, that heavily impacted Windows devices all over the world. The end result of this was a “Boot Loop”. This happens when the device restarts itself again for no apparent reason after the first boot up sequence has been initiated. Because of this, the device cannot cycle all of the way through, and as a result, it will not display the usual desktop that the end user is accustomed to seeing all of the time.

Was this an actual Cyberattack?

Because it was deemed to be caused by a rogue piece of content that was ingested and deployed to customers all over the world, it was not deemed to be a true Cyberattack. But very serious questions still remain about this, and in fact, other Cyber professionals are even giving second and third thoughts if this was in the end launched by a Cyberattacker.

But no matter how it stands, the fact still remains that various Cyberattacking Groups did take full advantage of this precarious situation, and thus, used this as their venue to launch the Threat Variants of their own design and making. For example, many kinds and types of Remote Access Trojans (also known as "RATs"), were launched. This can be technically defined as follows:

> A remote access Trojan (RAT) is a tool used by cybercriminals to gain full access and remote control on a user's system, including mouse and keyboard control, file access, and network resource access. Instead of destroying files or stealing data, a RAT gives attackers full control of a desktop or mobile device so that they can silently browse applications and files and bypass common security such as firewalls, intrusion detection systems, and authentication controls.
>
> (https://www.proofpoint.com/us/threat-reference/remote-access-trojan)

Also, hundreds of both Social Engineering and Phishing Attacks were launched as well, and to make matters even worse, there were well over 180 malicious domains that were registered with websites created on them, purporting to be offering timely information on how to recover from this massive fiasco. But these were phony websites, which lured the victim in by asking them to provide their confidential and private information and data, making a global nightmare even that much more worse.

Another form of Social Engineering Attack that was launched was that of fake Tech Support Calls. Whenever a system or a device goes down, it is always human nature to be initially in a state of panic and feel very vulnerable. This is the very moment that the Cyberattacker makes they move, in order to take full advantage of the emotional state of the victim.

Such is the case of the Crowd Strike Supply Chain Fiasco. In this particular instance, the most prevalent Threat Variant was that of the “Dolos-3PC”.

This is where the Cyberattacker creates and launches various types and kinds of Threat Variants with creative images, in an effort to induce engagement on part of the victim. This can also be done via Pop Ups, which seem to appear out of nowhere in a web browser. that encourage consumer engagement. The end result is that device of the victim is taken by many Pop Ups claiming, which involves a sense of urgency to call a phony technical support number.

The victims of the Crowd Strike Supply Chain Fiasco

It is important to note that were thousands of victims in this incident. It wasn’t localized to just one geographic area, rather it impacted almost everybody around the world, even just individuals with a home computer. Here is a sampling of the victims:

- The major international airlines of the world included the following:
  - American Airlines
  - Delta
  - KLM
  - Lufthansa
  - Ryanair
  - SAS
  - United Airlines
- The major international airports.
- All kinds and types of financial institutions
- Healthcare including most GP surgeries and many independent pharmacies

- The Media Industry
- The Retail Industry
- The Hospitality Industry
- The Sports Industry
- Apart from the international airlines, the other parts of the Transportation Industry mostly the railroad companies.

The efforts taken by Crowd Strike

Given the size, scope, and magnitude of this fiasco, it is of no surprise that Crowd Strike would thus come under the microscope to take proactive action their part in order mitigate the damage that was already done. First, they totally eradicated the update, which was done in a couple of hours. Second, Crowd Strike created very detailed Incident Response and Disaster Recovery Plans so that if this same fiasco were to happen again, there are at least a series of documented steps that can be taken quickly. In this regard, there is often confusion as to what these two are. The former deals with mitigating the Threat Variant immediately, and the latter focuses upon bringing up the mission critical processes and operations of the impacted business as quickly as possible. Then there is also the Business Continuity Plan, which focuses on the long term recovery of the business, back to where it was before being impacted.

Other pertinent steps that CrowdStrike has taken includes the following:

- Developer testing of the source code.
- Conduct ress testing, fuzzing, and fault injection exercises.
- Content interface testing, in order to make sure that there are no rogue pieces of content, which was the culprit in the first place.
- There will also be real-time monitoring which will be conducted by the Falcon Sensor. As a fail safe, customers will have final control

downloading and deploying their own software updates and patches. At the end of the fiasco, Crowd Strike claimed that 97% of the impacted Falcon Sensors had been fully repaired.

Because Microsoft was the first to be blamed for the Crowd Strike Supply Chain Fiasco, it would only be natural for them to come to take immediate action, as it was reviewed earlier in this chapter. First, they almost instantaneously deployed their own team of experts in an effort to work directly with impacted customers on service restoration of their devices.

Second, Microsoft had also collaborated with both Google Cloud and Amazon Web Services (AWS) in order to alert them and to mitigate any kinds or types of impacts that would be felt by impacted customers on both of these respective Cloud Platforms.

Third, Microsoft took both legal and technical actions in order to ensure that Crowd Strike, or for that matter, any other Third-Party Supplier would not possess the ability to deep dice into its core Operating System or any other related offerings in both M365 and Azure.

The impacts on Cybersecurity Insurance

One of the first thoughts that came to all of the impacted victims was how they could financially recover from all of the downtime and losses that had occurred. The only way that this could be done was to file a claim with their respective insurance carriers, assuming that the victims actually had some sort of Cybersecurity Insurance. But it is very important to note here that simply filing a claim is not an absolute guarantee of getting a financial payout. Insurance companies today have become very stringent, and require that their applicants as well as policy holders maintain and uphold the strictest levels of what is known as “Cyber Hygiene”.

Here examples of some of these:

- If you are the business owner, you must fill out a lengthy questionnaire attesting truthfully that you have all the controls in place to protect the PII Datasets. Also, you must provide evidence that you have taken steps to address the gaps and weaknesses in your IT/Network Infrastructure. This is typically done by either conducting a Penetration Test or a Vulnerability Scan.
- After you have the above, in most cases, your questionnaire must be certified by an outside third party that you trust or with whom you have worked in the past.
- After you have submitted all this stuff with your application, the insurance company can still come on site to your place of business and conduct a random audit to make sure that what you have attested to is correct.

But along with the above, there are other alarming statistics as well, such as the following:

- From 2018 to 2022, premium rates have gone up year over year.
- In 2023, 79% of United States businesses experienced a dramatic increase in premiums.
- SMBs with less than 250 employees were likely to be denied any kind of coverage, if they filed a claim.

Steps to be taken to help guarantee a payout in the face of another Crowd Strike Supply Chain Fiasco

There are a number of strategies that any individual or a business can take, and these are as follows:

1. *Understand Risk*:

Risk is a very subjective term to define, and depending upon the industry, it can have different kinds of meanings. But for Cybersecurity, at least in my view, this metric represents how much downtime your business can take (because of a security breach) before you start to incur some real financial losses. The best way to do this is to conduct a detailed Risk Assessment Analysis, to take an inventory of and categorize both your physical and digital assets. Once you have done this and have ranked each one to their degree of vulnerability, you will have a much better idea of what your actual Risk Posture is. Also, the insurance company will look at this and see how it compares to the overall average in the Cyber Industry. If you find that your Risk Posture is overall too high numerically, then you will want to take the steps to bring it down before you apply for any Cyber Insurance. Of course, the more that you can lower it, the better the chances that you will be given a policy.

2. *Understand the Contract*:

   If you have been lucky enough to be awarded a policy, you will first receive a contract. It is imperative that you review in detail over and over again. Cyber Insurance can be very tricky to understand, and the coverage will vary greatly. Of course, you will be covered for the direct costs that you incurred because of a security breach, but the very murky areas are after the fact, such as paying legal fees in case your lawsuits, regulatory fines, reputational/brand damage, etc. Although I am by no means an insurance expert, my best advice is to hire a really good lawyer that can review the contact inside and out, and have him or her negotiate the terms of it with the insurance company so that it will be much more favorable to you. You do not ever want to file a

claim and have it rejected because it was not covered by your contract!!!

3. *Pay Attention to Compliance*:
   More than ever before, businesses in both the United States and the European Union are coming under very close scrutiny of the Data Privacy Laws, most notably those of the GDPR, CCPA, HIPAA, etc. As a result, the insurance company that you have applied to for a policy will want to make sure that you have taken every effort to mitigate the risk of being audited by any of them. The primary reason for this is that the financial penalties can be quite steep, and the insurance companies do not ever want to pay out such a huge amount if a claim was filed under this circumstance.
4. *Create the Plan*:
   At the very minimum, you should create an Incident Response Plan. This is one of the very first items that an insurance carrier will request proof of. Of course, it would also be quite beneficial to also create and show that you have a Disaster Recovery Plan and a Business Continuity Plan deployed as well and is being rehearsed on a regular basis.
5. *The Outside*:
   It is equally important to prove to the insurance carrier that you have very carefully vetted out your Third-Party Suppliers, and that they too are following your stringent Security Policies, especially when it comes to protecting the Personal Identifiable Information (PII) datasets that you have entrusted them with.

Examples of legal actions taken in the wake of the Crowd Strike Supply Chain Fiasco

As a result of this incident, there were quite a number of lawsuits that were filed against Crowd Strike. But two most notable ones are as follows:

1. *The Actual Owners*:
   In this case, this would be the actual shareholders of the company. In this lawsuit that was filed, the shareholders claim that Crowd Strike made false and misleading statements about the accuracy and the validity the software testing procedures it has deployed. They also claim the share price of Crowd Strike tumbled greatly after the incident. The shareholders want financial repayment for the value Crowd Strike stock shares that fell between November 29, 2023, and July 29, 2024.
2. *The Delta Air Lines Lawsuit*:
   This was filed by the airline on Delta Air Lines on October 25, 2024, over severe downtime that was faced. The damages incurred by Delta exceeded over $500 million, and they also sharply accuse Crowd Strike of severe negligence that led to a global catastrophe. In its counter legal argument, CrowdStrike in turn sued Delta that the downtime incurred by the airline was their own negligence, by not taking up the help and support that was offered to them by Crowd Strike

The lessons learned from the Crowd Strike Supply Chain Fiasco

Just like in any type or kind of security breach that has been launched by a Cyberattacker, there will always be lessons learned from it which can be applied to the future. A lot of this information and data can be gleaned after a detailed Digital Forensics Investigation has been completed. But what is even more paramount is these so-called Lessons Learned must be shared

with employees, customers, and key stakeholders that have been impacted by it. In this regard, the “Lessons Learned” should point directly how to have better “Cyber Hygiene Habits”. In terms of the IT Security team, these “Lessons Learned” become of paramount importance, as they need to learn what happened and develop a set of Best Practices and Standards to mitigate the same Threat Variant (or a different version of it) from impacting the business again.

So, now the main question is: what has been learned from the Crowd Strike Supply Chain Fiasco? Here are some examples:

1. *The Need for Backups and Failover*:
   Failover systems can be classified Redundant Systems, and Data Centers are located in different geographical segments. These guaranteed that uninterrupted operations during outages will still continue, whether it was intentional or accidental. A prime example of this is when the business has their entire IT and Network Infrastructure in Microsoft Azure. From here, they select a primary Data Center, and even select others as backup, which are even located in different countries. So if the primary Data Center fails, the business can then roll over the next Data Center and continue normal business operations like nothing has ever happened.
   In terms of backups, it is absolutely imperative that the CISO and their respective IT Security team maintain a regular backup schedule, with backups store on site, and even in different geographic locations as well. In this regard, there are three types of backups that can be made:
   - The Full Backup: This is where entire backups are created of the databases on a regular basis.
   - The Incremental Backup: This is where information and data are backed up which are only new, which were entered into the

databases from the last Full Backup.

- The Differential Backup: It is also like an Incremental Backup, but it will not copy over the new information and data that have been entered into the Database. Rather, it will keep doing this on a real-time basis every time it has been initiated.

2. *Making Use of Existing Frameworks and Playbooks*:
   It is not known if Crowd Strike actually used any established Cyber related Frameworks or not, but it is highly recommended for the CISO and their IT Security team to use them, especially those that are available from the NIST and CISA. Also, it is highly recommended that a business make use of and deploy what are known as "Cyber Playbooks". These are technically defined as follows:

   > A cyber security response playbook is a plan you develop that outlines the steps you will take in the event of a security incident. Most organizations keep their incident response plans very simple and then augment specific types of incidents with cyber response playbooks.
   >
   > (https://cofense.com/knowledge-center/what-is-a-cyber-response-playbook/)

   The good news here is that many of them can now be automated, through the power of Generative AI. So for example, if a business were to be hit by a Threat Variant, the incident response that is detailed in the Cyber Playbook can be triggered in order to contain the breach within a matter of minutes. More detailed information about creating and deploying a Cyber Playbook can be accessed at the link below:
   https://cyberresources.solutions/Supply_Chain_Book/Playbook_CISA.pdf

3. *The Tail Risk*:

   The Tail Risk can be technically defined as follows:

   > The concept of tail risk entails the notion that some risks could bring down organizations, or in extremely rare circumstances, entire industries.
   >
   > (https://www.paloaltonetworks.com/cybersecurity-perspectives/the-long-tail-of-cyberthreats-part-i#:~:text=The%20concept%20of%20tail%20risk,financial%20markets%20around%20that%20time)

   As it has been reviewed throughout these sections on Crowd Strike, the fiasco that happened literally brought down businesses to their knees, taking to days to recover. The prime example of this is Delta Airlines, especially with their lawsuit. The bottom line here is that when the CISO and their IT Security team model what potential Threat Variants could look like, they need to take into account these extremes as well.

4. *Redundancy*:

   This was addressed just earlier, but in this case, Crowd Stike solely relied upon the Orion Platform for deploying the software to the thousands of clients. Rather than using just one with such a large geographic span, it is highly recommended that they should use multiple ones, but each serving only one, particular geographic location. That way, if one Platform goes arwy, the geographic impact will be much more limited in nature. The reliance upon just one Platform is also sometimes referred to as a “Mono Culture”.

5. *The Crisis Management*:

Apart from having the Incident Response, Disaster Recovery, and Business Continuity Plans in place and being practiced, it is absolutely imperative that the CISO and their IT Security team maintain an open line of communications with all employees, customers, and key stakeholders in the time of a security breach. Also, accountability must be held and enforced. One of the best ways to do this is to have and maintain a 24 × 7 × 365 hotline so that all forms of communications take place. This is also referred to as "Crisis Management".

6. *The Phased Rollout*:
   Probably one of the biggest lessons to be learned is the importance of deploying software patches and updates in a gradual, "phased" fashion. Of course, this will not stop a Supply Chain Attack from actually happening, but at least it should help to greatly mitigate the amount of damage that could potentially happen. In other words, it should help to reduce what is known as the "Cascading Effect". In fact, a good methodology is as follows:

   Initial deployment to a small, diverse subset of systems
   Monitoring for unexpected behaviors or conflicts
   Gradual expansion to larger groups
   Maintaining the ability to rollback if problems arise quickly.

   (https://ipkeys.com/blog/lessons-from-crowdstrike/#:~:text=The%20CrowdStrike%20incident%20exposed%20the,problems%20before%20they%20become%20widespread)

Other well-known Supply Chain Attacks

Apart from the Solar Winds Supply Chain Attack and the Crowd Strike Supply Chain Fiasco, there have been a number of other “notable” events, and they are as follows:

1. *The Discord Bot Platform Attack*:
   This happened in March of 2024. Thia particular Cyberattacking Group has primarily targeted the GitHub Software Repositories. They did this by distributing malicious Python packages, and other forms of Malicious Payloads.
2. *Okta*:
   This happened in October of 2023. They are one of the world’s largest IAM Providers, and it was discovered that the Cyberattacking Group was able to access the Personal Identifiable Information (PII) datasets of both customers and employees. They were also able to gain access to Okta’s Customer Relationship Management (also known as a “CRM”) databases.
3. *Microsoft*:
   This occurred in February of 2023. In this case, the Cyberattacking Group used what is known as a “Binary Repository Manager”. It can be technically defined as follows:

   > Binary repository managers store, manage, and version binaries and artifacts and their metadata. These are different from source code repositories.
   >
   > (https://www.releaseteam.com/binaries-artifacts-and-packages-oh-my/)

   Microsoft has used them to store various components of its software components, especially those used in Azure. By injecting malicious

pieces of Malware, the Cyberattacking Group was able to penetrate deep into the IT and Network Infrastructure of Microsoft, thus allowing them to hijack confidential corporate information and data.

4. *Norton*:
   This happened in May 2023. Norton is perhaps the largest producer of Anti Virus Software packages in the world. In this case, the Cyberattacking Group took advantage of the vulnerabilities that were found in the "MOVEit transfer" software package that transfers files from one location to another in a secure manner. In the end, they were able to infiltrate into the IT and Network Infrastructure of Norton, and were able to steal the Personal Identifiable Information (PII) datasets of just the employees. They also threatened to launch Extortion Attacks if a huge ransom payment was not made.
5. *Airbus*:
   This happened in January of 2023. In this case, an account belonging to an employee of Turkish Airlines was compromised. From this, the Cyberattacking Group was able to covertly heist the Personal Identifiable Information (PII) datasets of well over 3,000 Airbus Third-Party Suppliers; some are most notable such as Rockwell Collins and the Thales Group.

In summary, this chapter has provided a deep dive into two of the worst forms of a Supply Chain Attack, Solar Winds and Crowd Strike. Also, the lessons learned from both incidents were also provided. Also, other Supply Chain Attacks were reviewed as well. In the next chapter, we will review some ways in which a CISO and their IT Security team can overall mitigate the risk of a Supply Chain Attack from happening to them.

Chapter 4

How to mitigate the risks of Supply Chain Attacks

DOI: 10.1201/9781003585916-4

So far in this book, the chapters have covered the following topics:

- An overview into Cybersecurity
- A review of Supply Chain Attacks
- An deep dive into the two major Supply Chain Attacks – Solar Winds and Crowd Strike

In this chapter, we look at some ways in which the threat of a Supply Chain Attack can be *mitigated*. Note the emphasis on the last word. There is no such thing as being 100% immune from a security or a Threat Variant. Any individual or business can be, but the trick is reducing the statistical odds that you any of them will actually become a victim.

In this case, any business can be impacted by a Supply Chain Attack. The goal is then how to reduce those chances from happening, and if it does, how quickly can once bounce back from it. The latter is often referred to as "Cyber Resiliency", and it can be technically defined as follows:

> Cyber resilience is the ability of an organization to enable business acceleration (enterprise resiliency) by preparing for, responding to, and

> recovering from cyber threats. A cyber-resilient organization can adapt to known and unknown crises, threats, adversities, and challenges.
>
> (https://www.opentext.com/what-is/cyber-resilience)

In this regard, one of the best ways that a business can mitigate the risks of a becoming a victim of a Supply Chain Attack is deploy what is known as the "Zero Trust Framework", also known more commonly as just "ZTF".

The Zero Trust Framework

The Zero Trust Framework can be technically defined as follows:

> Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
>
> (https://www.crowdstrike.com/en-us/cybersecurity-101/zero-trust-security/#:~:text=Zero%20Trust%20is%20a%20security,access%20to%20applications%20and%20data)

Put in simpler terms, the Zero Trust Framework assumes that nobody can be trusted under any circumstances, and that everybody must go through constant levels of verification of their respective identities. Thus, the motto of the Zero Trust Framework has become the following:

> "Never Trust, Always Verify"

There are different ways of deploying an actual Zero Trust Framework, but the idea is to break away completely from the concept of "Perimeter Security". This is where there is only line of defense that encircles the business. While it may be heavily fortified, there is only one layer of it. So, if the Cyberattacker can break through this, they can get free reigns of the entire IT and Network Infrastructure of a business.

So with this in mind, the ultimate aim of the Zero Trust Framework is to break out the IT and Network Infrastructure of a business into different segments or "zones". Each one of them has their own layer of defenses, which is primarily driven by the use of Multifactor Authentication, also known as "MFA" for short. This is where there at least three or more different authenticating mechanisms that are used to confirm the identity of the individual wishing to gain access into it.

An illustration of the Zero Trust Framework can be seen in Figure 4.1.

Figure 4.1 An example of the Zero Trust Framework. (https://www.shutterstock.com/image-photo/zero-trust-security-concept-businessman-using-2521369195)

The next sections of this chapter does a deeper dive into the Zero Trust Framework.

What is impacted by the Zero Trust Framework

Apart from just employees, there are also key components from within your business that have to be put under the scrutiny of the Zero Trust Framework. These include the following:

1. *All Sorts of Devices*:
   This includes everything from hard wired servers to workstations and even all forms of wireless devices. You want to make sure that only legitimate devices are accessing your network infrastructure and not rogue ones, such as when employees using their personal Smartphones to access the shared resources.
2. *Software Applications*:
   With pretty much all of your employees now working from home, it is even more difficult to tell than ever before if they are using legitimate applications that have been authorized by your IT Security team. In this regard, you need to confirm that any application trying to access your servers are the real thing or not.
3. *Your Data*:
   It is the data that you store, use, and collect on a daily basis that literally forms the lifeblood for your business. This include everything from your Intellectual Property (IP) all the way to the Personal Identifiable (PII) datasets of your employees and customers. Because of this, you do not want anything to fall into the hands of a Cyberattacker. Thus, it is absolutely imperative that only legitimate people gain access to this, which spells out the need for many layers of authentication to take place first.

4. *Your Overall Infrastructure*:
   Many people associate the Zero Trust Framework with just the digital component of your business. But it also includes the physical infrastructure as well. For example, if an individual needs to gain access to a server in your data center, they should be completely vetted first. This also includes going through at least three layers of authentication. For instance, this could include a smart card, entering a unique ID number, as well as submitting to a Biometric modality such as that of Fingerprint and/or Iris Recognition.
5. *Your Network Infrastructure*:
   Gaining access into a network line of communications and moving laterally from there is one of the most common ways in which the Cyberattacker utilizes in order to break through your lines of defense. Therefore, not only do you need to make sure that all unknown vulnerabilities are remediated, but also that only legitimate employees can initiate a path of network communications. As the Zero Trust Framework mandates, your Remote Workforce should be given only those rights and permissions that they need to perform their daily job functions, which is also referred to as the "Concept of Least Privilege". Also, the Framework further establishes that your network infrastructure should be divided into smaller segments, which are known as "Subnets". Therefore, if the Cyberattacker can break through one layer of authentication, the statistical odds that they will break through the others becomes greatly diminished.

The advantages of the Zero Trust Framework

There are a number of strategic advantages to it, which are as follows:

- *You Are Exposed to a Lesser Degree of Vulnerability*:

By assuming nobody can be trusted, you are actually decreasing the threat surface for the Cyberattacker to penetrate into. Also to a certain degree, you are also at a much-lowered level of risk of an Insider Attack from precipitating.

- *You Will Have a Varied Mix of Authentication Mechanisms*:
  Using more than one layer of authentication does not mean that you use different forms of it. The Zero Trust Framework mandates that you make utilize entirely different mechanisms, which was eluded to earlier in this article.
- *Other Areas of Your Business Will Also Be Segmented*:
  Apart from your network infrastructure, there will be other aspects which will also have to further divided as well, such as the data that you store. For instance, rather than storing it all in just one On Prem database, you will have to contain them in different ones. In this scenario, you may even want to make use of a Cloud-based platform such as that of the AWS or Azure. You can create different instances of databases, and you can quickly and easily deploy many authentication mechanisms quickly and easily.

How to deploy the Zero Trust Framework

Deploying this takes a lot of planning and should be done in a phased in approach. The following are key areas that you need to keep in mind as you deploy it:

1. *Determine the Interconnections*:
   In today's environment, your digital assets are not just isolated to themselves. For example, your primary database will be connected with others, as well as to other servers, which are both physical and virtual in nature. Because of this, you also need to ascertain how these

linkages work with another, and from there, determine the types of controls that can be implemented in between these digital assets so that they can be protected.

2. *Understand and Completely Define What Needs to be Protected*:
   With Zero Trust, you don't assume that your most vulnerable digital assets are at risk. Rather, you take the position that everything is prone to a security breach, no matter how minimal it might be to your company. In this regard, you are taking a much more holistic view, in that you are not simply protecting what you think the different potential attack planes could be, but you are viewing this as an entire surface that needs 100% protection, on a 24 × 7 × 365 basis. So, you and your IT Security team need to take a very careful inventory of everything digital that your company has, and from there, mapping out how each of them will be protected. So rather than having the mindset of one overall arching line of defense for your business, you are now taking the approach of creating many different "Micro Perimeters" for each individual asset.
3. *Crafting the Zero Trust Framework*:
   It is important to keep in mind instituting this does not take a "One Size Fits All" approach. Meaning, what may work for one company will not work for your business. The primary reason for this is that not only do you have your own unique set of security requirements, but the protection surface and the linkages that you have determined will also be unique to you as well. Therefore, you need to take the mindset that you need to create your framework as to what your needs are at that moment in time, as well as considering projected future needs as well.
4. *Implement how the Zero Trust Framework Will Be Determined*:

The final goal to be achieved is how it will be monitored on a real-time basis. In this particular instance, you will want to make use of what is known as a Security Information and Event Management (SIEM) software package. This is an easy to deploy tool that will collect all of the logging and activity information, as well as all of the warnings and alerts and put them into one central view. The main advantage of this is that your IT Security Team will be able to triage and act upon those threat variants almost instantaneously.

Project management requirements for the Zero Trust Framework

Here is what you need to take a careful look at:

1. *You Need to Determine What Needs to be Protected*:
   One of the fundamental concepts behind the Zero Trust Framework is that your entire IT and Network infrastructure has to be broken out into different segments. In a way, this can be compared to the establishment of subnets. Although the overall goal is to have a 100% breakdown, this may not be feasible, depending upon your security requirements. For this reason, you need to work with your IT Security team and carefully map out what really needs to be protected, and how it can be further divided. But it is also important to keep in mind that that this will not be a static analysis. Rather, it will be a dynamic one, and it should be scalable. For example, if your IT/Network infrastructure grows or shrinks over time, the Zero Trust Framework that you deploy has to follow in tandem with this. Also, just don't take a macro view. You need to take a micro one, because you will be dividing things up, and each layer of separation will require its own needs and attention. This kind of approach is also known as "DAAS",

which stands for critical *D*ata, Software *A*pplications, Digital *A*ssets, and *S*ervices.

2. *Determine How Your Data Flows*:
   This is something that we normally take for granted. But with the Zero Trust Framework, you have to take all the time that is needed to carefully map out how your data flows from within your IT/Network infrastructure. The reason for this is that since you will be segmenting it, you need to make sure that there will still be a clear and seamless flow for the data packets. In other words, you don't want them blocked off at one point and not be able to reach the other segment. Also, by doing this kind analysis, you and your IT Security team will get a clearer idea of the kinds of controls could be potentially needed, and how best they should fit strategically.
3. *Create a Tentative Model*:
   Once you have determined what needs to be protected and how best the flow of communications will be between segments, the next step is to actually formulate a working model of your Zero Trust Framework. It is very important to keep in mind that at this stage, there is no one size fits all approach. You need to create it according to your own security needs. For example, at this stage, one of the key items that you need to look at are the type of authentication mechanisms that will be needed, and where they should be placed so that they best support the controls that will be implemented. With this methodology, Multifactor Authentication (MFA) is an absolute must. This means that you must implement at least three or more tools in order to fully confirm the identity of an end user. Further, they must also be different in nature, according to the following:
   - Something you know

- Something you have
- Something you are.

For example, a password could be used for the first, an RSA token could be used for the second, and a Biometric could be used for the third. Meaning, the end user has to present all three pieces before they will be granted access to the shared resources. Another key item to remember is that each segment in the Zero Trust Framework should not repeat the same authentication sequencing from the previous layer. To illustrate this, the second layer should consist of a set of challenge/response questions, a smart card which contains more detailed information about the end user, and a different Biometric modality. Finally if you are able to implement even more than three authentication mechanisms, which will even provide a greater level of security.

4. *Creating the Policies*:

   Another key element of the Zero Trust Framework is the creation of the Security Policy that creates the foundation for it. It should at minimum consist of the following to enforce yet another layer of security:

   - Which end users should be accessing what resources
   - An audit log of the resources and applications that are being logged into
   - The times of the day in which shared resources can be accessed
   - Implementing the Next Generation Firewall to allow even more advanced filtering and blocking of malicious data packets.

5. *Daily Monitoring*:

   Once you have a working model of your own Zero Trust Framework, you should now deploy it. But do not do all of this at once, rather a

phased in approach should be used. For example, rather than deploying all of the authentication mechanisms for each segment, do them one at a time. That way, if any unforeseen issues come up, they can be worked out in a much more efficient and manageable fashion, rather than dealing with them all at once.

The key provisions of the Zero Trust Framework

Most organizations are adopting the usage of MFA, because the more layers you have, the statistical probability of a Cyberattacker breaking through each successive wall of defense greatly diminishes. In fact, MFA is one of the key tenets of the Zero Trust model, and there are others as well, which include the following:

- *The Cyberattacker Is Always Present*:
  This tenet asserts that there is always the strong possibility that a Cyberattacker is lurking from both outside and inside of the environment of your IT infrastructure, even if evidence points to the contrary.
- *The Implementation of Least Privilege Access*:
  As it states, the IT Security team of any business should only grant those privileges, accesses, and rights that are the bare minimum needed for an employee in order to accomplish and execute their daily job functions. Any escalation in this would have to go through an intensive review process.
- *The Use of "Micro Segmentation"*:
  In this regard, the lines of defenses that are used to protect the IT infrastructure of your business are broken up into smaller zones. So, instead of having just one wall, it is further broken down into smaller, micro walls, to provide a more layered approach. For example, with

the former, once a Cyberattacker penetrates it, all of your mission critical assets are exposed, but with the latter, not everything is completely exposed if the Cyberattacker breaks through. Thus, this gives you the critical time that you need in order to quickly isolate and remediate any breaches that may occur.

Also, micro segmentation means that of all of the network shared resources are allocated into separate, secure zones as well. For example, while an employee may have the privileges to gain access to the accounting files, he or she will required to obtain an entirely new set of login credentials in order to gain access to the files of the other departments in the company.

- *The Adoption of a Software Driven Approach Is a Must*:
  Keeping a Zero Trust model finely tuned means that it needs constant attention, on a daily basis. If an IT Security team were to do this manually, it would take an enormous amount of time, and mistakes can very be made very easily. Therefore, making use of an automation platform that is software based is also key component. You can easily create the micro segments that are needed (as described above), and all updates and policy enforcements can be done on a real-time basis, quickly and efficiently. In this kind of scenario, Artificial Intelligence (AI) technology is starting to be used to a larger degree.
- *The Need for Easy to Access Dashboards and Analytics*:
  While micro-segmentation does have its key benefits, it does suffer from downside: More smaller entities means that it can be harder to keep track of all of the activity that is transpiring from within the IT infrastructure as a whole. Because of this, the Zero Trust model also calls for the deployment of easily accessible Dashboards and Analytics that can consolidate all of this into a quickly decipherable “View”. The

idea here is that the IT Security team can then garner a holistic picture of what is going on and thus be able to react to any anomalous or malicious behaviors with a proactive mindset.

Other methods to reduce the risk of Supply Chain Attacks

Apart from the Zero Trust framework, there are also other ways in which a CISO and their IT Security team can mitigate the risk of a Supply Chain Attack from happening to their business. Here are some other strategies:

1. *Use Honeytokens*:
   This can be technically defined as follows:

   > A honey token is data that looks attractive to cyber criminals but, in reality, is useless to them. Generally speaking, a "honey" asset is a fake IT resource created and positioned in a system or network to get cyber criminals to attack it. In this way, honey tokens are similar to honeypots.
   >
   > (https://www.fortinet.com/resources/cyberglossary/honey-tokens)

   In other words, you are actually baiting the Cyberattacker to go after datasets that look real, but have no legitimate value to them. In essence, you are also creating what is known as a "Honey Pot" to lure more Cyberattackers in. By doing this, one will be able to glean quite a bit of valuable information and data as to how they operate and infiltrate into their targets.
2. *Secure PAM*:

This is an acronym that stands for “Privileged Access Management”. This was too was reviewed earlier in this book, and essentially these are the super user privileges, rights, and permissions that are assigned to a more senior job title. For example, a Network Administrator would obviously have much more escalated rights, permissions, privileges than would an Administrative Assistant. The bottom line here is that these kinds of accounts that are created are a prime source of prey for the Cyberattacker, and once they have access to it, they can use them to launch even more devastating Supply Chain Attacks with a more cascading effect, thus affecting more victims on a global basis.

3. *Assume the Worst*:

   As it was also reviewed earlier in this book, the CISO and their IT Security team should not only be proactive, but they should also assume the worst case scenarios in their Threat Modelling. In other words, they also need to include various kinds and types of Supply Chain Attack scenarios so that they create their Incident Response, Disaster Recovery, and Business Continuity Plans accordingly.

4. *The Insider Threat*:

   This kind of Threat Variant is possibly one of the hardest to detect, because it typically involves the employee or a contractor of a company that has intimate knowledge of the IT and Network Infrastructure of the business that they work in. It is very important to remember that Supply Chain Attacks do not simply come from the outside environment, they can also originate from within the internal environment as well. One of the best ways to mitigate this kind of Threat Variant in happening is to have a 24 × 7 × 365 hotline, which should be anonymous, so that anybody can report on a confidential basis any abnormal behavior amongst other employees or contractors.

5. *The Shadow IT*:
   This is another kind of Threat Variant that mostly uses the tactics of Social Engineering. It can be technically defined as follows:

   > Shadow IT is the use of IT-related hardware or software by a department or individual without the knowledge of the IT or security group within the organization. It can encompass cloud services, software, and hardware.
   >
   > (https://www.cisco.com/c/en/us/products/security/what-is-shadow-it.html)

   In simpler terms, this when an employee deploys a software application onto their device in order to conduct daily job tasks. But, this particular application has not been approved by the IT Security team, and thus, it can pose a huge risk. The primary reason for this is that leaves a backdoor wide open for the Cyberattacker to infiltrate into, and launch a Supply Chain Attack. Also, since the particular software application has not been tested in a sandboxed environment, it could also pose a serious violation of the Security Policies that are in place.
6. *The Third Party Supplier*:
   This concept was also reviewed in detail earlier in this book, but apart from the vetting aspect of it, the CISO and their IT Security team also need to keep assessing the risks that the Third Party Supplier brings as well. This is can very be accomplished by conducting a Risk Assessment Analysis of the controls that they have in place which are used to protect the datasets that you have entrusted them for processing, storage, and archiving. Doing this is particularly important

if they are storing them in a Cloud-based environment, such as that of the AWS or Microsoft Azure.

7. *The DevSecOps*:
   This is an acronym that stands for "Development, Security, and Operations". This is where members from each three of these teams come together to make sure that the source code that has been created for a Web-based application is free from any known gaps, vulnerabilities, or weaknesses. It is very important for the CISO and their IT Security team to implement this kind of methodology, as any backdoors in the source code which have not been closed can also be easily penetrated by the Cyberattacker in order to launch a Supply Chain Attack. *This should also include testing the Open Source APIs before they are used in the source code!!!*
8. *The Patches and Upgrades*:
   This is probably one of the most proactive steps that the CISO and their IT Security team can take. This simply means that they need to be on a constant vigilance for the latest software patches and upgrades that come out from the vendors that they work with, and deploy them on a timely basis. *But of course, it is absolutely imperative that they be tested in a sandbox environment first before they are released into the Production Environment!!!!*

For more preventative strategies, access the link below:

http://cyberresources.solutions/Supply_Chain_Book/Supply_Chain_CISA.pdf

Finally, this chapter has reviewed has reviewed some of the major strategies that the CISO and their IT Security team can take in order to mitigate the

risks of a Supply Chain Attack happening to their business. In the end it takes, both a proactive mindset on their part and technology to make this happen. The cardinal rule is that one simply cannot rely upon one side too much.

Index

Pages in *italics* refer to figures.