Breaking Down What Cybersecurity Insurance Is All About

By Ravi Das

Introduction

In today's environment, there is no doubt that the Cyberthreat Landscape is constantly evolving and changing on a daily basis. It seems like that hardly one threat vehicle is launched, there are many variants of it that will soon follow. A perfect example of this is Phishing. This is probably one of the oldest forms of a Cyberattack, but yet, it is still being used heavily today in many different variants, such as that of Spear Phishing and Business Email Compromise.

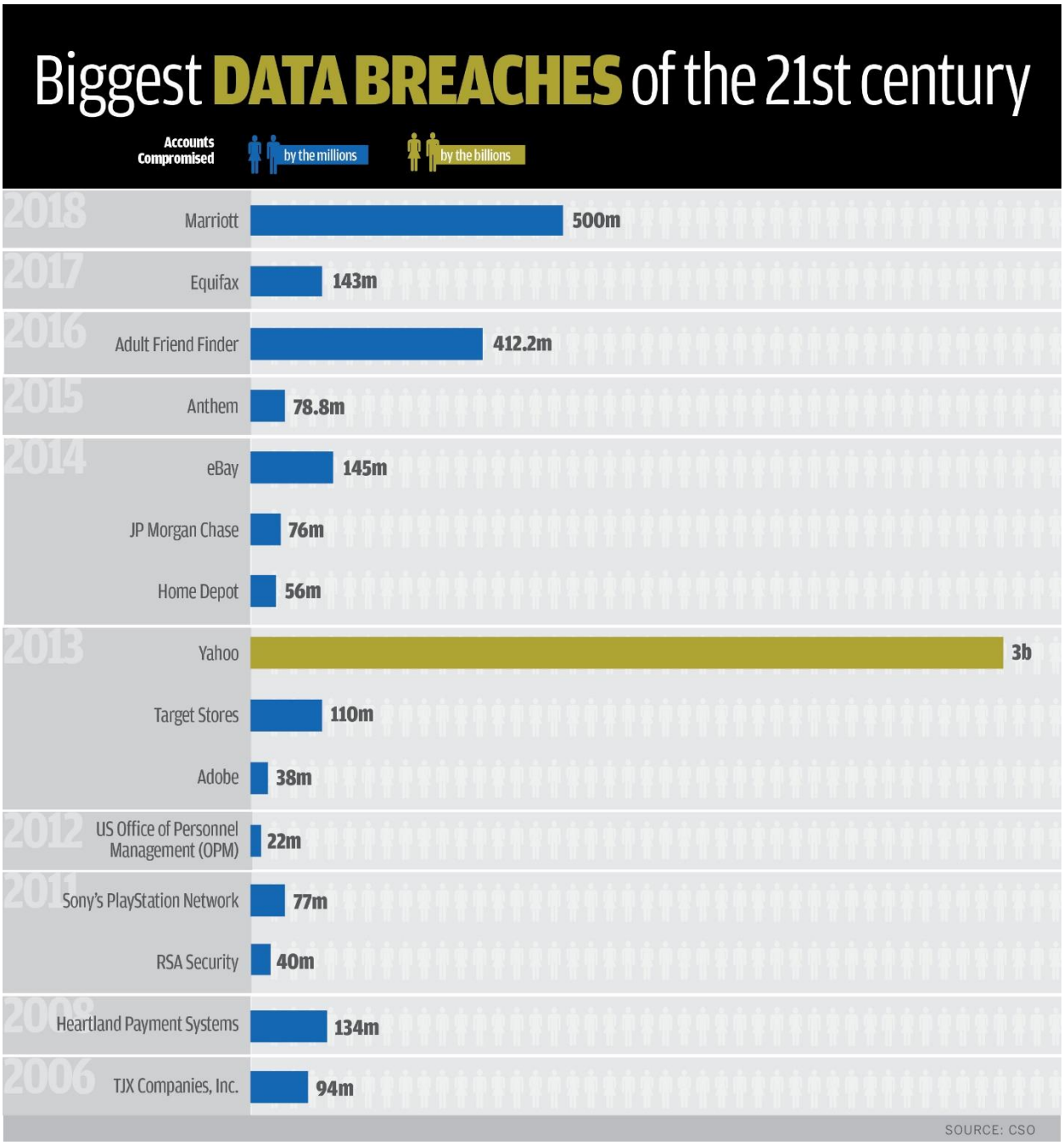
In a way, this can be compared to that of cat and mouse chase. The cat is the Cyberattacker, and the victim is the mouse. The goal here of course is to stay one step ahead of the cat, but it seems like the cat has the advantage in this case. The bottom line is that a Cyberattack is real, and it can have devastating effects to a business or a corporation.

For example, once an organization has been impacted, there is downtime that is experienced in order to restore back to a baseline level of operations, so that mission critical processes can keep running. Then there is the loss of revenue experienced because of this. But these are only the ***tangible*** losses.

Beyond this, there are also the ***intangible*** losses. These are the unquantifiable losses, which include the following:

- Tarnished brand image;
- Loss of reputation;
- Loss of customers;
- The time it takes new customers;
- The time it takes to send out notifications to customers and the stakeholders (both Internal and external) that their Personal Identifiable Information (PII) could be at risk;
- The time it takes to answer questions posed by law enforcement and regulators (both at the federal and state levels);
- Any further downtime that may experienced in a potential lawsuit.

Here are some examples of what the latest Cyberattacks have cost Corporate America:



(SOURCE: 1)

As one can see from the diagram above, the costs are enormous, and are only getting worse year after year. But keep in mind that these are only the tangible costs, not the intangible costs. If the latter were to be factored, the costs would be of course, much more staggering.

Because of this, Corporate America is now looking into procuring Cybersecurity insurance as means to hedge, or cover the losses incurred after a Cyberattack. However, purchasing a plan is a little bit more complicated that it is when getting car or medical insurance, and it is poorly misunderstood by the C-

Suite. Therefore, the goal of this white paper is to provide an overview into Cybersecurity Insurance, focusing upon the following:

- What Cybersecurity Insurance is, and its history;
- The advantages and disadvantages of Cybersecurity Insurance (what is covered and what is not);
- The factors that insurance companies consider when providing coverage;
- What you need to take into consideration when deciding upon an insurance carrier;

What Cybersecurity Insurance Is & Its History

In its broadest sense, Cybersecurity Insurance can be defined as follows:

"A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event." (SOURCE: 2).

Cybersecurity Insurance is not a new product by any means. It actually has its roots going back to the late 1970's, when the Errors and Omissions concepts were first introduced. The first versions of Cybersecurity Insurance came out in the 1980's, which were primarily designed to help the losses covered by the large financial firms and other Fortune 500 companies.

But it was not until the late 1990's when interest in Cybersecurity Insurance policies started to grow in the marketplace. The primary catalyst for this growth were the fears of Y2K, which were cemented in the thoughts that there would be widespread computer shutdowns on a global basis. In this regard, it has been the Lloyd's of London which has been credited with offering the first true Cybersecurity Insurance policy.

This initiative was launched by Keith Daniels and Rob Hamesfahr, former attorneys at the law firm known as Blatt, Hammesfahr & Eaton. The underwriters for this first policy were Ian Hacker (who was an underwriter at Lloyd's of London), Ted Doolittle, and Kinsey Carpenter. The primary goal of this policy was to offer 3rd party coverage for major business interruptions.

It should be noted that during this time frame, there was no 1st party coverage offered. Also, these first types of Cybersecurity Insurance did not cover losses experienced by Insider Attacks caused by an employee with malicious intents, failure to come into compliance with any federal rules and regulations, and any fines or penalties that could be imposed onto a business entity by a regulatory body.

It was after the 9/11 attacks that interest in Cybersecurity Insurance spiked even further. This was because many leaders, both at the corporate and government level, were starting to realize the gravity of Cyberattacks. In this instance, the first types of threat vehicles were those of Trojan Horses, Viruses, and primitive forms of Malware.

Because of this, there was also the stark realization that it is not just physical attacks that can cause business interruptions, but threats launched towards the virtual world could also bring an organization down to its knees. This type of loss was not covered by Cybersecurity Insurance during that time frame. The primary for reason for this was that there was no historic data in which to calculate and measure and price this kind of risk. As a result, many insurance providers focused most of their offerings to those losses that were incurred by attacks to physical IT and Network Infrastructures.

But as Cyberattacks continued to mount and proliferate upon the Cloud (or Virtual) Infrastructures, the demand for Cybersecurity Insurance policies to cover this type of loss started to grow, because of the sheer amount of Identity Theft and Data Breaches that were occurring.

Another catalyst that finally made the insurance industry to cave in and to extend their policies to cover these kinds of losses was the passage of the "California Security Breach Information Act of 2003".

This law mandated that any entity which conducted business transactions in the state of California had to notify any customers if they were Personal Identifiable Information (PII) was at risk because of a Cyberattack which occurred.

Many other states also passed and implemented similar laws rather quickly, and even the European Union passed similar laws as well with a major focus upon the telecom providers and Internet Service Providers (ISPs).

Because of all of this, the major insurance carriers now offered 1st party coverage to businesses and corporations (this includes such things as Forensics Investigations, Public Relations damage and repair, credit monitoring services offered to victims, and costs associated with notifying people that they may have been impacted).

But despite this, not all the insurance carriers during this time frame offered the same type of coverages to Corporate America. For example, many of the carriers had extremely strict sub limits still set into place, and the amounts that were paid out differed greatly.

One of the biggest reasons for this was that each carrier had varying risk tolerances that were willing to take on, and different methodologies in quantifying what level of risk was deemed to be acceptable and too much. After all, insurance providers are businesses themselves, and they want to make sure that they don't to take on too much of a burden if it is going to directly impact their bottom line.

The turning point that made the insurance carriers loosen their strings was the horrific security breach that occurred at the retail giant known as TJ Maxx. In this attack, over 45 million credit card and debit card numbers were stolen, which cost the company almost $5 Billion. Over 25 class action lawsuits were filed, and the retailer had to doll out $177 Million in settlement claims. Even to this day, this Cyberattack has been deemed to be one to one of the worst in history.

To top this off, there were also those security breaches at Anthem Blue Cross Blue Shield and Target, in which over 10 Million credit card and debit card numbers were heisted. This only showed that despite the best lines of defenses that were being implemented, any business or corporation is at risk for a large scale Cyberattack. Thus, at the present time, the demand and need for a comprehensive Cybersecurity Insurance policy is at its highest point ever.

The Advantages & Disadvantages of Cybersecurity Insurance

This section of the whitepaper examines what a typical Cybersecurity Insurance policy covers (the advantages), and what it does not cover (the disadvantages).

<u>The Advantages</u>

Here is what is typically covered:

1) Any damage or loss to Electronic Data:

   This includes any "damage, theft, disruption or corruption" to the Electronic Data that a business or corporation may possess. It even covers any loss or damage to your employee's workstations, laptops, or wireless devices. But in order to be provided coverage, there are two criteria that need to be met:

   - The Electronic Data that has been impacted must be the result of a Cyberattack;
   - Coverage will only be granted to the Electronic Data that resides on company issued devices.

   This provision will also provide coverage to recover any hijacked, lost, or stolen Electronic Data, and even the costs that are associated with hiring a specialist to accomplish this task.

2) Any lost income or expenses experienced by a Cyberattack:

   To a certain extent, many insurance providers will provide for any monetary loss as a result of a Cyberattack, whether it is lost revenue or extra expenses incurred because of it. However, this coverage is typically different than the normal coverage afforded by a standard Commercial Property Policy, which applies to only any monetary losses incurred to the physical property of a business entity.

3) Losses from Cyber Extortion:

   This can be specifically defined as follows:

   "Cyber extortion is the act of cyber-criminals demanding payment through the use of or threat of some form of malicious activity against a victim, such as data compromise or denial of service attack."

   (SOURCE: 2)

   Ransomware is a typical example of this. Under this kind of Cyberattack, the hacker sends out Malware to your computer or server, which will lock up the screen, and any other mission critical files that resides within it. The hacker will typically ask for a ransom, made payable by using a virtual currency, such as Bitcoin. Theoretically, once this is paid, the Cyberattacker should send you the decryption algorithm to decrypt and unlock your screen and files, but in reality, this hardly ever happens. Cybersecurity Insurance will cover this, from two perspectives:

   - Any costs that are associated with responding to the Cyberattacker;
   - Any ransom money that you have paid them.

4) Costs of Notification:

   After a security breach has impacted an organization, many regulations now require for the C-Suite to provide written notification to the affected stakeholders, which typically involve the customers, suppliers, etc. Cybersecurity Insurance will cover the following:

   - The costs that are associated with notifying the stakeholders (such as letter preparation, the costs of sending the letters out, etc.);

- Any legal expenses;
- Providing credit monitoring services to the impacted stakeholders (this is typically for one year);
- In some cases, the costs that are associated with setting up a temporary call center in order to address stakeholder questions and concerns.

NOTE: The above are known as "First Party Coverages" and are subject to a deductible based upon the type of Cybersecurity Insurance that you have.

It should be noted that Cybersecurity Insurance also provide for what are known as "Third Party Coverages", and these typically arise from claims that been filed by the impacted stakeholders against the organization, and any type monetary settlements that have been subsequently agreed upon. Typical examples of this include the following:

1) Network Security Liability:

   These kinds of claims arise when lawsuits are filed against a business entity when there has been a major breach, and the Personal Identifiable Information (PII) has been hijacked, as a result of a Distributed Denial of Service (DDoS) attack, Virus, Malware, or any unauthorized access to the database in which the PII resides in.

2) Network Privacy Liability:

   This is different than the above, in which the Cybersecurity Insurance policy will cover any claims on the grounds that the organization did not adequately protect the PII that was stored on the database. In adequate protection often refers to not deploying and applying the latest software patches and upgrades, letting unauthorized users gain access to the database when there was no need for them to in the first place, etc.

3) Electronic Media Liability:

   Typical examples of this include:

   - Copyright Infringement;
   - Domain Name Infringement.

   Cybersecurity Insurance will only cover those instances if the above has been published and distributed maliciously over the Internet, without your prior knowledge.

The Disadvantages:

Here is what is typically NOT covered:

1) Anything in excess of your policy limit or sublimit:

   Any costs or claims that have been filed that exceed your current Cybersecurity Insurance policy will not be covered. In these cases, if more coverage is needed, you will have to get a newer policy, which means it will be more expensive. A sublimit can be specifically defined as follows:

"A limitation in an insurance policy on the amount of coverage available to cover a specific type of loss. It places a maximum on the amount available to pay that type of loss, rather than providing additional coverage for that type of loss."

(SOURCE: 3)

For example, a sublimit may on the costs that are related to a Forensics Investigation, which would place cap for that specific kind of activity.

2) Loss of Intellectual Property (IP) or corporate Trade Secrets:

At the present time, Cybersecurity Insurance does not cover this, because the industry cannot quantitatively gauge with certainty any losses that occur because of a devaluing in this area.

3) Loss to reputation and brand damage:

The insurance industry has no current financial methodology quantify the risk in these two areas. The present view is that it is up to the CIO or CISO to provide protections in this, as well as any financial expenses that are incurred.

4) Expenses due to Business Interruptions or Downtime:

In this instance, any loss monetary loss incurred is not covered by a Cybersecurity Insurance policy.

5) Any security breaches that have been caused by negligence:

The insurance industry will not provide coverage for an organization that maintains a level of poor "Cyber Hygiene". Although this is a qualitative term, this can stem from such things as not implementing a Security Policy, being out of compliance with regulatory agencies within the federal government, or even failure to maintain minimum standards that have been set forth by the insurance company that is providing the Cybersecurity Insurance.

6) Threats posed by Nation State Actors:

This can be specifically defined as follows:

"They work for a government to disrupt or compromise target governments, organizations or individuals to gain access to valuable data or intelligence and can create incidents that have international significance." (SOURCE: 4).

Insurance companies do not provide coverage for any hacks or Cyberattacks that have been ascertained as terrorist by nature. Typically, this will involve the Fortune 100 companies, that have a large international dominance, with a lot of Personal Identifiable Information (PII) at risk.

7) Remediating IT Assets:

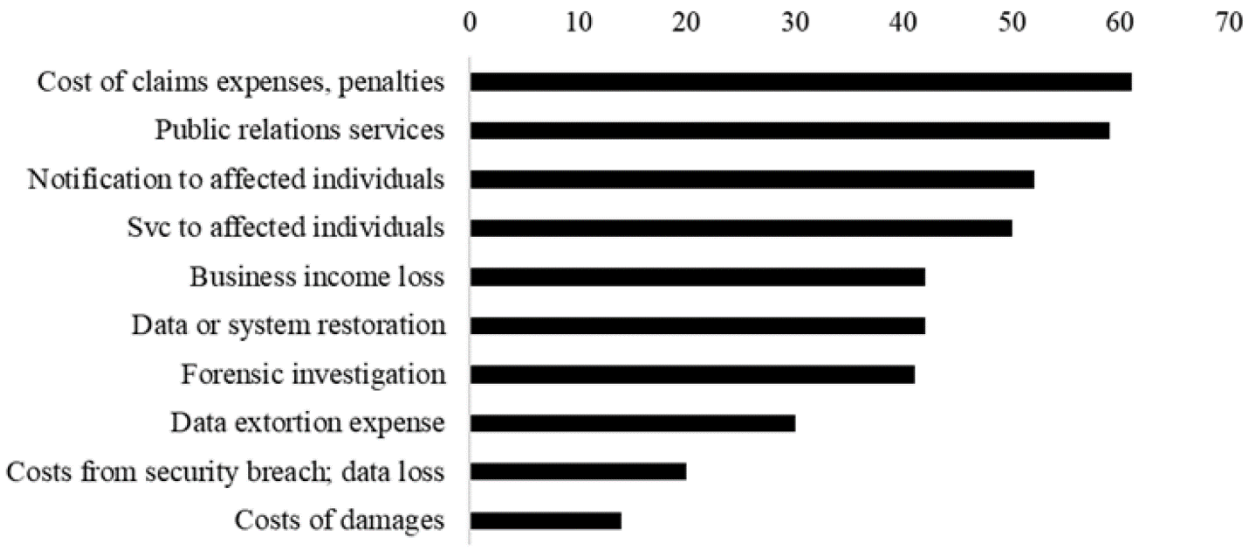
Any costs that are incurred to make an IT Asset more fortified after a Cyberattack is not covered.

8) Losses occurred to Physical Property:

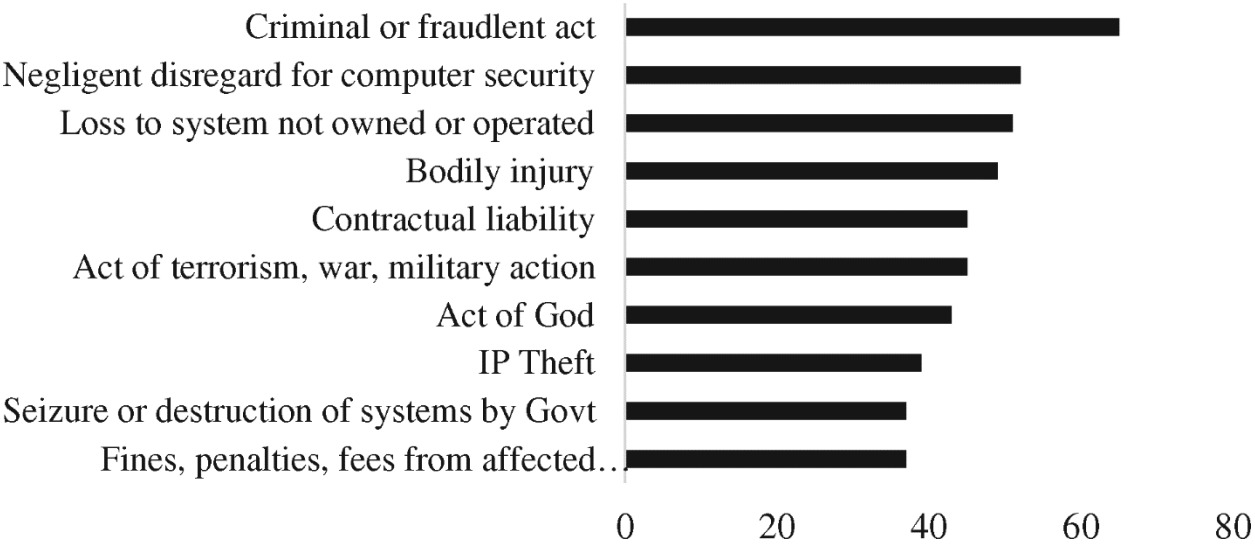
As described earlier, Cybersecurity Insurance will typically cover only those losses that are deemed to be digital in nature. Thus, in this regard, any expenses incurred to the Physical Property of an organization will not be covered. So, for example, if there was a Cyberattack that damaged the Critical Infrastructure to a city (such as the water supply, electrical power grids, oil/gas pipelines, etc.) these would not be covered.

The following two illustrations pictorially depict what is covered and what is not by a Cybersecurity Insurance policy.

What is covered:



What is not covered:



(SOURCE: 5).

It is important to note at this point that the insurance industry is often criticized from two fronts:

- There are currently no efforts being undertaken to create quantitative financial models or developing other risk assessment tools so that more coverage, especially in the way of the intangible losses can eventually be offered to businesses and corporations.

- Insurance companies are only providing Cybersecurity Insurance to make themselves more profitable. For example, according to a recent study by the Financial Times demonstrated that in 2017, the Loss Ratio (which is the monetary number of claims paid divided by the monetary amounts of premiums that have been paid in) was as high as 32%. For example, for every $1 Million in premiums that are being paid by an organization, only a mere $320,000 is being paid out in claims.

  (SOURCE: 6).

The Factors That Insurance Companies Consider When Providing Coverage

When deciding upon when to award an applicant with a Cybersecurity Insurance policy, many insurance carriers take a close look as to what the organization is already doing in terms of fortifying their lines of defense.

These are all qualitative measures, because as it has been pointed out throughout this whitepaper, there are currently no known financial models or other types of assessment tools in the insurance industry that can quantify the level of risk that an applicant possesses. At the present time, here is what a typical insurance company looks at before giving out a Cybersecurity Insurance policy:

1) <u>If perimeter security has been installed</u>:

   Typically, this includes a mixture of the use of Firewalls, Routers, and Network Intrusion devices. The insurance company wants to see that the organization has taken a proactive approach in deploying these tools to protect both their IT and Network Infrastructures.

2) <u>Making sure that there is a Security Policy in place and that it is being enforced</u>:

   Although this is one of the first items that any business or corporation should address for their own sake, this is one of the of key areas that gets looked at when an application is submitted for a Cybersecurity Insurance policy. An insurance company wants to see that it is being updated on a regular basis, and that ***<u>all employees</u>*** are abiding by the rules that have been set forth by it.

3) <u>The implementation of a robust Password Policy</u>:

   It is important to note that passwords are often the first target that the Cyberattacker will go after. After all, once he or she has this prized possession, they literally have the keys that can unlock the proverbial “crown jewels” of the unsuspecting victim. In fact, in many of the recent Cyberattacks, organizations have been blamed for enforcing poor Password Policies. Because of this, many insurance carriers are now scrutinizing business entities to make sure that have an airtight Password Policy in place. Typically, this is what they look for:

   - Making sure that passwords are reset at regular intervals;

- Confirming that the passwords used are very difficult to crack;
- Employees are constantly trained in how to create a strong password.

In this instance, in order to meet the stringent requirements of the insurance industry, it is best if the organization has deployed the following:

- Multifactor Authentication: This is where another layer of security (such as the use of Biometric Technology), in addition to the password, is being used to fully authenticate the employee before they gain access to shared resources on the network drives;

- The use of a Password Manager: These are software applications that instantly create very long and complex passwords that are very difficult to break, and even resets the passwords used at regular intervals, without any intervention required by the employee.

4) Confirming that there is a regular schedule for the deployment of software patches and upgrades:

   Even when organization does this, there is still no guarantee that their servers, workstations, wireless devices and other software applications won't be hit by a Cyberattack. But by doing this on a timely basis, it proves to the insurance carrier that the C-Suite is taking a very proactive stance in making sure that their systems are continually being updated.

5) Making sure that the network lines of communications between remote workers and the corporate headquarters is secure:

   This is another area that is a prime target for the Cyberattacker. If they can intercept any sort of communications in this fashion, then more than likely, he or she will be able to gain subsequent access through a backdoor in the IT or Network Infrastructure of an organization. As a result, insurance companies also take a close look as to what kinds of preventative measures have been taken so that this does not happen. Key areas that are looked at include the following:

   - Has a Virtual Private Network (VPN) been installed?
   - Is Two Factor Authentication (2FA) being used? For example, along with the password, is another security measure being used to authenticate the remote employee, such as an RSA Token?
   - What are the standards of Encryption that are deployed?

6) The types of Physical Access Controls that have been installed:

   As it has been pointed out to earlier in this whitepaper, any security breaches caused to the physical premises of a business or a corporation are not covered by a Cybersecurity Insurance policy. But still, the levels of physical security that have been deployed by an organization are carefully looked at by the insurance carrier before a policy is awarded.

If the business entity meets or exceeds the above, then there is a good probability that it will be accepted as a policy holder by the insurance carrier. But it is also important to keep in mind that once this has occurred, the C-Suite needs to be proactive in maintaining their lines of defense, as an insurance company can conduct an in-depth audit at any point in time, they feel it is necessary.

Typically, this involves the following:

- Incident Response and Disaster Recovery plans are being practiced on a regular basis and the appropriate documentation is updated in real time when and as needed;
- Security Awareness Training, especially for employees, are being taught on a regular basis as well;
- Any known and unknown gaps and vulnerabilities are being continually being remediated. This is typically done by conducting an exhaustive Penetration and/or Threat Hunting Test;
- Making sure that there are an adequate number of controls in place in order to protect the Personal Identifiable Information (PII) and/or other types of regulated data that the organization has been entrusted with to store in their databases;
- Making sure that the business entity is up to speed in terms of compliance with both federal and state regulations;
- There are no repeated patterns of any security related issues not being addressed and corrected.

By being proactive with the above, the C-Suite can more or less be guaranteed that they will receive the full amount of their claim after is has been filed.

What You Need to Take into Consideration When Deciding Upon an Insurance Carrier

Just as much as insurance companies take a very detailed and comprehensive look at their applicants before awarding a Cybersecurity Insurance policy, the C-Suite also needs to scrutinize the insurance company as well before they decide upon a carrier. Here are some key variables that need to be taken into consideration with this:

1) <u>What are the different kinds of Cybersecurity Insurance policies that are available</u>?

   Because of the dynamics of the Cyber Threat Landscape, insurance companies are now being forced to offer more than just one type of policy. If possible, try to obtain a standalone policy, as this will provide far more comprehensive coverage that just simply attaching an add on to an existing policy. But even more important, make sure that whatever Cybersecurity Insurance policy you intend to get is not only customizable to your specific needs at the present time, but also into the future as well.

2) <u>Confirm the deductible amounts</u>:

   As you are comparing the various Cybersecurity Insurance policies that you are interested in, make sure that you take careful notice of the deductible amounts as well. In fact, this process is almost the same when you evaluate medical and car insurance policies. Stay from the notion that paying a cheaper premium is always the best. Truth to be told, it is not, and in the end, you literally get what you pay for.

3) <u>Carefully examine who is covered specifically by the Cybersecurity Insurance policy</u>:

   Today, many organizations are relying upon the use of outside, 3rd parties in order to keep up and stay ahead of their production schedules. But it is important to keep in mind that if you rely upon an external 3rd party, and if they are impacted by a Cyberattack, ultimately, you will be held responsible for any financial losses that have been incurred. Therefore, it is very important

to make sure that you can include such 3rd parties as well into your Cybersecurity Insurance policy, so that you can be covered in this regard as well.

4) What kinds of Cyberattacks are you protected from:

As we all know, there are many kinds of Cyberthreats that exist today, and when you include the variants of them, the list multiplies by at least 100X. Therefore, you need to make sure that the Cybersecurity Insurance policy that you are about to procure covers any and all kinds of security breaches that may occur, inclusive of its intentionality (for example, what is it malicious in nature, or was it simply a negligent error caused by an employee)? Make sure that Cyberattacks that are initiated by Social Engineering are as covered as well.

5) Make sure of the time frames in which your Cybersecurity Insurance policy starts and ends:

Many of the Cyberattacks that are occurring today take a much longer time to detect and mitigate than ever before (ranging from months to even years), given the stealthy and covert nature of the hacker. One of these is that of the "Advanced Persistent Threat", or "APT" for short. It can be defined specifically as follows:

"This an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data. The targets of these assaults, which are very carefully chosen and researched, typically include large enterprises or governmental networks. The consequences of such intrusions are vast, and include:

*Intellectual property theft (e.g., trade secrets or patents);

*Compromised sensitive information (e.g., employee and user private data);

*The sabotaging of critical organizational infrastructures (e.g., database deletion)

*Total site takeovers."

Sources

1) https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
2) https://www.cisecurity.org/blog/cyber-extortion-an-industry-hot-topic/
3) https://www.propertyinsurancecoveragelaw.com/2012/12/articles/insurance/are-you-covered-sublimits-can-sneak-up-on-unaware-policyholders/
4) https://www.baesystems.com/en/cybersecurity/feature/the-nation-state-actor
5) https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419
6) https://www.cpomagazine.com/cyber-security/businesses-are-finding-out-that-cyber-insurance-coverage-might-not-be-what-they-thought/
7) https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/
8) https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878
9) https://www.tandfonline.com/doi/full/10.1080/23738871.2017.1296878?scroll=top&needAccess=true
10) https://prowritersins.com/wp-content/uploads/2018/09/The-History-of-Cyber-Insurance-041316V1.pdf
11) https://www.thebalancesmb.com/what-s-covered-under-a-cyber-liability-policy-462459
12) https://www.darkreading.com/vulnerabilities---threats/10-things-cyber-insurance-wont-cover/d/d-id/1325123
13) https://www.hpe.com/us/en/insights/articles/cyber-insurance-what-companies-look-for-and-why-claims-get-rejected-1808.html
14) https://www.cio.com/article/3065655/what-is-cyber-insurance-and-why-you-need-it.html