Cybersecurity Risk Management:

Why It Is Needed and How to Proceed

Table of Contents

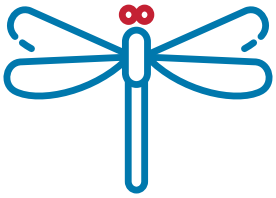
Cyber threats are among US CEOs' top concerns, according to PwC's 20th Global CEO Survey. According to a recent McKinsey survey, 75% of experts consider cybersecurity to be a top priority for their businesses, but only 16% say that their companies are well prepared to handle an actual cybersecurity risk. Awareness of the magnitude and scale of cyber threats is indeed growing, but **executives still find the challenge of cyber risks overwhelming and confusing,** with plenty of uncertainty about what to do and how to handle a cybersecurity breach.

In this article, we will evaluate the current cyber threat environment, learn how to avoid the common pitfalls of building a cybersecurity plan, and find out how to effectively establish the company's first line of defense from cyberattacks – a cybersecurity risk management plan.

Rising level of cyber threats

According to Cybersecurity Ventures, cybercrime is expected to cost the world $6 trillion annually by 2021, more profitable than the global trade of all major illegal drugs combined. Ransomware attacks are reported to be the top cybersecurity threat to organizations today, according to a recent study from Verizon, and are now targeting business-critical systems causing financial harm, downtime, and reputational damage.

Some of the most alarming and most notable attacks include:



Dragonfly Attacks on energy companies in the US, Canada, and Europe, revealing their alarming capacity to disrupt operations and damage a company's reputation.

WannaCry ransomware attacks on telecommunications and logistics companies, as well as some companies from the public sector.

NotPetya ransomware attacks on major companies from different industries in Europe

It wasn't just small companies that were victimized by NotPetya and WannaCry; even large, well-prepared firms were affected. This only proves that even with sensible preparation, no one is completely safe from the damage that untargeted malware attacks can cause.

In 2012, FBI Director Robert S. Mueller, III expressed a strong statement saying, "There are only two types of companies: Those that have been hacked, and those that will be hacked." By 2015, Terry Greer-King, Director of Cybersecurity, Cisco UKI & Africa, updated this statement with: "There are effectively two types of companies today; those that have been hacked, and those that don't know they have been hacked." These statements just go to show that cybercrime is a real and increasingly serious concern for all types of businesses today.

Exacerbating these concerns is the rising popularity of the Internet of Things (IoT) and its inevitable avalanche of products and production systems that will be hooked up to the internet. It is expected that by 2020, IoT may comprise as many as 50 billion devices, many of which will most likely have inadequate security or no security at all. This means that the number of potential entry points for hackers will rapidly reach alarming levels across all industries, and with it, an exponential increase in risk.

> "There are only two types of companies: Those that have been **hacked**, and those that **will be hacked**."
>
> **Robert S. Mueller, III,** Director, FBI

How to address the alarming level of cyber risks

All organizations, regardless of size and industry, are likely to be confronted by a wide range of different cyberattacks of varying frequency, complexity, and impact daily. But organizations can do something to prevent, or at least mitigate, these cyberattacks; they can start by preparing by familiarizing themselves with the common pitfalls of setting-up and having a cybersecurity risk management plan, and then, devise a more proactive and collaborative approach that is suitable for their organization.

a) Start by understanding and addressing common pitfalls

Delegating problem to IT / CISO

A lot of organizations treat cyber risk as a technical issue and leaves it all for the IT department or the Chief Information Security Officer (CISO) to deal with and resolve. Cybersecurity may be a technical problem at its core, but defending a business is different from simply protecting its servers. Security has to be embedded across the whole business, and no longer just simply an IT component. Defending a business requires an understanding of a company's business model, value chain, the relevant risks to be faced, the roles and responsibilities of each person involved, and proper governance. Given this, IT alone will not be enough to handle cybersecurity since it affects and encompasses all these business aspects.

Throwing resources at the problem

According to a survey conducted by AT&T, 65% of organizations believe that their internal cybersecurity measures are adequate to protect them against cyber threats, yet 80% had been victims of a successful cyberattack in the previous year. Most companies are confident that their cybersecurity risk management plan will be able to protect them, when they follow a checklist that is used or is recommended by other companies.

The problem with this approach is that it doesn't take into account what the current level of protection and vulnerability a company hasand does not establish nor consider what the goal is for setting-up the organization's risk management program. They purchase state of the art malware detection systems, antivirus software, and network firewalls for protection even if these acquisitions don't suit the company's needs and address the company's vulnerabilities.

Organizations are usually given a limited budget for cybersecurity risk management, and it is important for each one to be able to know where and how to spend it right. With this, Bob Chaput, CEO of Clearwater Compliance, challenges organizations with the question: *"Am I going to spend my*

cybersecurity budget on somebody else's list of 'good things to do?' Or am I going to spend it on the basis of my organization's assets, my exposures, my business goals and objectives?"

The fragmented, one-size-fits-all checklist approach may have been recommended, or may have worked in the past, but organizations need to keep in mind that cyber threats are all ever changing and ever evolving, and a company's cyber risk management plan must also keep up with that level of innovation and development.

Apart from simply following a checklist, other companies, on the other hand, try to persuade high-profile hackers to be part of their company and rely on them to set-up the company's cyber threat defenses. The problem with this approach goes back to the pitfall of simply delegating the management of all cyber risks and threats to a single persona, when it must very well be the responsibility of each and every employee (and all other third-party partners) to be aware and accountable for their own operations and functions.

Treating the problem as a compliance issue

There are a lots of existing cybersecurity protocols, frameworks, and checklists that are being recommended by other organizations. But these solutions are tailored to their organizations; which means that even if it is working for them, it doesn't guarantee that it can protect your organization from future cyberattacks. Their company's cyber risk and vulnerabilities may be entirely different from yours.

The easy, traditional response of blindly following a checklist has proven inadequate in the growing landscape of cyber risks and threats today. To keep up with the times and counter the growing threat of cybercrime effectively, companies should accommodate the growing complexity of corporate networks by constantly assessing their cybersecurity posture.

Other concerns that puts your company at risk

Other related pitfalls that are the most common reasons why cybersecurity often breaks down in companies include:

- The company not having an inventory of the company's digital assets
- The company not knowing or not taking note of which third parties it digitally connects with
- The company not identifying who is most likely to come after its data
- The company not resolving or not patching up known system vulnerabilities
- The company having a wide attack surface, without having security plans in place
- Employees not being oriented or trained on their role in security

b) Devise a more proactive, collaborative approach

A more proactive and collaborative approach to cyber risk not only helps alleviate costs, but it also enables companies lessen the disruption of operations that current cybersecurity initiatives often bring about. McKinsey has derived the following cybersecurity principles from their experience working with some of the world's leading cybersecurity players:

- Cyber risk needs to be treated as a risk management issue like any other complex, critical, nonfinancial risk
- It needs to be addressed within a business context
- Cyber risk needs to be dealt with on multiple levels
- It calls for adaptive defenses
- Cyber risk calls for holistic, collaborative governance

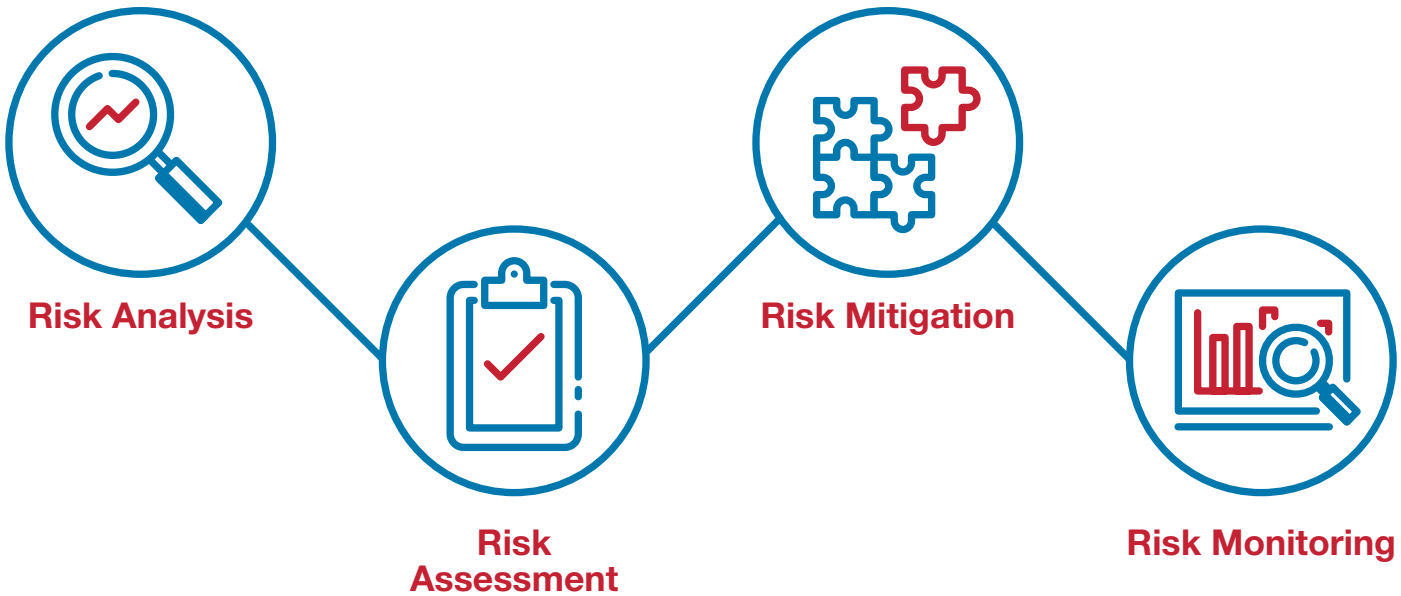
According to McKinsey, companies that adhere to these principles tend to be much more resilient to most attacks than other companies, and they generally utilize their cybersecurity resources and funds better. Prioritizing investments on crucial assets alone are reported to help save up to 20% of cybersecurity cost. Incorporating these principles in setting-up your company's cyber risk management plan can significantly improve your company's cyber health and posture.

How to set-up a cybersecurity risk management plan

Different companies face different kinds and different levels of threats depending on the industry and other company-specific factors (such as size and structure of the organization). There is no single approach for building one's cyber risk management plan. But if your company is starting from scratch and doesn't have a cybersecurity risk management strategy in place yet, the National Institute of Standards and Technology (NIST) Cybersecurity Framework is said to be a good reference point.

Even with a standard framework like the NIST's, it is still recommended for companies to tailor their security controls and processes to the unique needs of their specific business industries or functions. For example, the healthcare industry, apart from the typical financial fraud, experiences crucial unique risks like the possibility of medical insurance fraud and attacks on computer-controlled medical devices (e.g. pacemakers, insulin pumps, continuous glucose monitors, etc.). Medical devices have moved from analog care solutions, to systems that require network connectivity and that operate under certain imposed limits from the manufacturer (as to what controls can and can't be applied to them). This is why the framework must be tailor-fit to every specific need of an industry or a business, so that critical concerns or provisions like these will be addressed.

Whatever industry, whatever function, and whatever framework you decide to go with, some important aspects, that are recommended to be a standard part of an organization's cybersecurity risk management plan include: 1) Risk Analysis; 2) Risk Assessment; 3) Risk Mitigation; and 4) Risk Monitoring.



a) Risk Analysis

PwC's 2017 Annual Corporate Directors Survey revealed that only 39% of directors are confident that they know their company has identified its most valuable and sensitive digital assets, and that around 25% had little or no faith at all that their company has identified potential threats and attackers.

The company cannot protect what it doesn't know. Which is why an important first step in setting-up a cybersecurity risk management plan is the Risk Analysis. It involves defining the relevant t hreats and attackers to the company, identifying the company's most critical assets, and assessing the company's current digital resilience and targeted level of cybersecurity. During this stage, organizations should focus more on getting the right information about the company's current state of cyber resilience and building relationships with the company's tech and security leaders, so that you can get a better sense of whether the company is doing enough.

Evaluate current cyber resilience and target level of cybersecurity

Companies need to obtain and evaluate the basic information on the company's own IT environment (and their cyber risk capabilities along their entire operation/value chain) and compare their own performance to that of industry benchmarks. Without this background, it's going to be hard to determine properly the level of risk the company faces. PwC recommends asking the following questions to help companies evaluate:

Regarding the nature of the company's systems

- Are they developed in-house, purchased and customized, or in the cloud?
- Are any of the systems or software being used, no longer supported by vendors?
- Is the company running multiple versions of key systems in different divisions?
- To what extent has the company integrated the systems of companies it acquired?

Regarding the company's existing security resources

- Where does IT security currently report?
- What are IT security's resources and budget? How do they compare to industry benchmarks?
- Has the company adopted a cybersecurity framework (e.g. NIST, ISO 27001)?

Based on these key background information on the company, organizations should set realistic goals for their targeted level of cyber resilience.

The company's goals should be guided by an objective and should be defined by measurable key risk indicators (KRIs) that is reasonable based on the company's current threat level and based on the standards of the industry that it belongs to.

Determine most relevant risks and threats

Before choosing and investing in a risk management plan, officers should strive to identify which risks are most relevant for their company. According to Difenda, a global leader in cybersecurity, risks must be **evaluated based on the probability of them happening** and **based on the impact** that they have on your company in order for a cybersecurity risk assessment to be effective. Only by a thorough assessment and prioritization of risks, can a company develop cost-effective strategies to manage the risks and improve their cybersecurity risk response. Some of the questions that executives may ask to guide them in the determining the most relevant threats are: How many and what types of cyber incidents do we detect in a normal week? or What is the threshold for notifying our executive leadership?

Identify your most critical assets

Knowing what to protect is the first step in creating an effective cybersecurity plan. The inventory scan should cover every asset that is connected that is connected to the corporate network (IT, OT, IoT), as well as people who have access to those networks (employees, suppliers, clients, service providers, etc.). The data from the asset inventory and people registry can be studied to help companies prioritize their security initiatives, as well as plan/strategize their response to attacks and recovery afterwards.

b) Risk Assessment

How does our own cybersecurity program and capabilities compare to that of industry standards and best practices? This is the guiding question for organizations in the next stage of setting-up a cybersecurity risk management, which is the Risk Assessment. It involves evaluating existing security and controls and assessing their adequacy relative to the potential threats of the organization.

After defining the company's most critical assets and determining its most relevant threats and attackers, preparing an appropriate response to risk requires the assessment of potential controls. Controls include all of the tools, tactics, and processes a company has to avoid, mitigate, share, transfer, or accept risk. This means that corporate structure, training and awareness programs, physical security, and other options should be considered in addition to traditional IT controls.

Identify and differentiate your controls

The main driver of cybersecurity waste and productivity loss is the forced implementation of the same controls across all assets of the company. Executives need to understand that not all assets require the same controls, and that there should be a distinction between the controls, based on the company's effective prioritization of assets and risks. The more critical an asset is to your company, the stronger and the more defined the controls for it should be. A few examples of strong controls would include a two-factor authentication and background checks of employees who will have access to the company's critical assets.

c) Risk Mitigation

IBM reports that the average cost of a data breach globally now stands at $3.86 million, a 6.4% increase from 2017. Given the high probability of a breach happening and the extent of the potential damage it has to a company's financial position and reputation, it's alarming that 54% of executives say that their companies still don't have cyber breach incident response plan in place.

The Equifax Data Breach

For instance, Equifax, one of the largest credit bureaus in the U.S., announced on September of 2017 that an application vulnerability on one of their websites led to a data breach that exposed about 147.9 million consumers**.** The company revealed in a statement that based on the company's investigation, the unauthorized access has most likely occurred from mid-May through July 2017. They have further reported that personal information (including Social Security Numbers, birth dates, addresses, and drivers' license numbers) of 143 million consumers and credit card data of 209,000 consumers has been accessed during the breach. Due to the extent of the damage brought about by the breach, CEO Richard Smith was forced to resign, two weeks after the public disclosure of the massive breach.

Several experts in the field of cybersecurity have also expressed their concerns and disappointment in how Equifax has handled the breach incident, some of them like Javvad Malik of AlienVault and EyalAharoni of Cymulate, even offered some insight as to how Equifax could have prepared and avoided cybersecurity breaches.

> "Companies like Equifax should know very well that **data is the lifeblood of the organization** and its crown jewels. As such, robust threat detection and response controls need to be implemented in order to thwart such attacks. Complimenting detection capabilities with threat intelligence and orchestration for response can help close out gaps, as well as speed up response times."
>
> **Javvad Malik,** Security Advocate, AlienVault

> "In this day and age, all organizations should expect cyber attacker/s to attempt to breach their security system especially those handling Private Identifiable Information (PII). For companies, like Equifax, that are dealing with extremely sensitive information—like social security numbers—there needs to be multiple barriers protecting that information from an attacker in case one of those barriers is breached. Companies also need to **constantly test and review their security posture** and how they are perceived from an attacker point of view and mitigate the vulnerabilities exposing them. Unfortunately, as seen in some cases such as this one, companies should also be prepared and have a plan on how they will handle a breach so that they can resolve the issue immediately and protect their customers from cyber attackers."
>
> **Eyal Aharon,** COO, Cymulate

Javvad Malik and Eyal Aharoni were only a few from a lot more cybersecurity experts that stated that the breach could have been avoided or could have been controlled better, if only Equifax had an effective cyber breach incident response plan in place, which they all doubt the company had based on how the company handled the situation. In lieu of this tragedy, cybersecurity experts remind companies to be constantly aware of the rising threat of cyberattacks, but to not be worried or overwhelmed, for there is something that can be done to prepare for and counter these kinds of attacks, and that to set-up a cyber breach incident response plan.

Set-up a cyber breach incident response plan

A good incident response plan outlines a flexible framework of the general steps that must be taken to **prepare for, respond to, and recover** from a security incident. An incident response plan must be **flexible enough to adapt** to the particular security incident the company is facing (e.g., network intrusion, denial of service, account takeovers, malware, phishing, loss of paper, employee data, security vulnerabilities detected by third parties, or theft of assets).

Some of the key elements that the cybersecurity incident response plan should detail include the following:

People

Assign the Internal Incident Response Team

- Identify team members from critical departments, describe their roles, and make sure you know who will provide you with the information you need to make critical decisions in the midst of an incident.
- Define the involvement and expectations from each department (communications team, finance leaders, business leaders, legal counsel and the broader crisis response team, as well as IT specialists

Specify the Third Party/External Relationships that must be established prior to an incident

- Identify key third parties that will assist the company and possibly facilitate smooth coordination of the incident response like external privacy counsel, forensics, crisis communications, media, mail and call center vendor, and credit monitoring.
- Cyber Insurance: Important to determine if the organization have cyber insurance and which level of incidents are going to be covered.
- Litigation: Some considerations include how the company will assess the potential litigation an attack leaves it with, or who will be able to assist them, if there are any recourse to the legal action.

Process

Include a process and procedure for every phase of the incident management lifecycle

- Provide a flexible framework for executing the eight key steps of incident response: (1) preparation, (2) identification, (3) assessment, (4) communication, (5) containment, (6) eradication, (7) recovery, and (8) post-incident.
- Experts from Booz Allen Hamilton, suggests that the plan should be supported by runbooks, which are tactical guides that address specific incident scenarios most likely to affect your business. Some examples include:

Cybersecurity Plans

How will the organization ensure it withstands the attack, isolates and assesses the damage done, and builds up defenses to prevent similar breaches in the future?

Business Continuity Plans

How will the organization continue to operate as normal while remedying the attack?

Compliance Concerns

What are the organization's duties for reporting the breach to the appropriate authorities, including law enforcement agencies if necessary, and how will these be discharged?

Public relations and communications

How will the organization communicate clearly and effectively with all potential stakeholders, including employees, customers, suppliers and investors, both directly and via the media where there is public interest in the breach?

Part of the publicity plans should cover breach notification and escalation procedures that should address the following:

- When will the board will be notified?
- What is the company's plan to inform regulators?
- How and when will other stakeholders (including individuals whose personal information may have been lost) be informed?

Technology

Technology aids the incident response process—from **vulnerability intake** to **understanding the security controls** on your electronic assets to **facilitating quick communication.**

At a basic level, there should be **automated process for incident handling**—if your organization is still using manual incident tracking systems, you are overdue for a technology investment.

Threat and vulnerability detection technology can **mitigate the impacts of a cyber breach.** Beyond basic, more sophisticated data analytics tools provide complex, customized statistics that can help measure the business impact of a breach, among other capabilities.

In practice, the cyber breach response plan is effectively a crisis management plan. It is required to provide guidance to every function of the organization involved in the response, set a level of understanding about what information is critical for senior leaders to know – as well as when and how to express it – and underpin the precision and the speed of the organization's continuous reaction as the breach continues to unfold – possibly over days, weeks or even months.

Promote education and awareness

Human errors are a significant contributor to the overall cyber risk that organizations face. In fact, 47% of business leaders say that human error (such as an accidental loss of a device or document, falling for phishing emails, clicking on links or downloading documents that turn out to be malware) had caused a data breach at their organization and had caused their company a lot of money.

The National Institute of Standards and Technology (NIST) recommends that cybersecurity risk management education be included in the onboarding process for employees and even business partners. It is extremely important for the business leaders to communicate their cybersecurity risk management plan to all employees and make sure they understand what is at stake and why it is important. Make sure that information and training are accessible and comprehensible to everyone, so that every employee knows who to call and what to do in case of a data breach.

PwC listed the following initiatives to help directors and employees to improve their knowledge of cybersecurity:

- Focus group discussions (assess the company's situation, current cybersecurity strategy, the types of cyber threats that face the company, and the nature of the company's critical assets)
- Attendance in external programs and conferences (that focus on the oversight of cyber risk)
- Ask law enforcement (e.g. FBI) and other cybersecurity experts to present on the current threat environment, attack trends, and common vulnerabilities.

d) Risk Monitoring

"How comprehensive is our cyber incident response plan?" and *"How often is the plan tested?"* are some of the questions that Davis Hake, Director of Cybersecurity Strategy for Palo Alto Networks Inc., recommends companies to ask, when monitoring and reassessing their cyber breach incident response plan. After establishing an incident response plan, PwC suggests that companies to constantly test and review the said plan in order to make sure that the processes are updated to keep up with the evolving industry trends and cyber threats.

Constantly review and revise the cyber breach incident response plan

It is important for companies to check on their cyber incident response and crisis management plan on a regular basis, in order for it to stay updated and relevant based on the threat environment and based on the company's needs. A company's incident response should be guided by a plan that has been tailored to the company's industry and fine-tuned through mock breach exercises.

The incident response plan is a critical element of the cybersecurity risk management strategy—not because it provides a prescriptive, detailed list of action items, but because it has been refined and practiced through tabletop drills conducted by the company itself, based on the data about its potential threats and attackers, its own control processes and capabilities, and its own risk management protocols.

Regularly hold plan testing and simulations

Regular plan testing and simulations through tabletop drills are essential to assess the clarity of assigned roles and responsibilities for everyone involved and as well as identify gaps in the mitigation and preparedness protocols. The board and other executives must be involved and must always ask what changes or modifications were made to the plan, as a result of the last simulation.

Apart from regular testing, the incident response team, and everyone involved, must always be aware of recent cybersecurity incidents that other organizations encountered, and advise them to update the company's controls or incident response plans based on those situations.

Conclusion

As cyber threats persist, more and more boards continue to recognize the need to step up and improve their knowledge of cybersecurity. Cybersecurity is no longer just an IT issue, but an imminent issue that should concern all functions of an organization. Setting up, continuously monitoring, and reassessing a cybersecurity risk management plan will be challenging and will take time, energy, and resources. But it assures your company's cyber health, security, and reputation in the long run.

Your cybersecurity risk management plan will be your first line of defense in recognizing and addressing potential threats and vulnerabilities. Investing in it and constantly working on improving it will not only protect your company, but it will also boost profits, meet compliance standards, reduce business liability, and help you gain a competitive advantage.