Ostrich Cyber-Risk

Four Ways for Executives to Better Understand and Mitigate Cyber Risk

Robert Shapiro
March 2022

*The opinions expressed here are my own personal opinions and do not represent the view of any company

Ostrich Cyber-Risk

Executive Summary

- The average cost of a cybersecurity breach in the U.S. is estimated at $9M, and is highest for Healthcare, Financial Services and Pharmaceutical organizations.
- Attacks are increasing in sophistication and originate from a variety of sources, including hacking communities, organized crime and state-sponsored actors.
- Cybersecurity audits are the foundation of a strong strategic plan, and should be performed regularly and proactively.
- Using the intelligence gained from an audit makes it possible to optimize budget allocation
- A combination of education, defense and insurance offers the best all-around defense against the potential devastating effects of an attack.

Introduction

There is no doubt that cybersecurity is a key business risk. It keeps many senior executives and board members awake at night, wondering if their companies will be victims of a major cyberattack—and the type of the destruction that results from such an attack.

Due to these high stakes, the cybersecurity industry continues to grow at unprecedented rates, from a value of $156 billion (USD) in 2020 to an expected $352 billion by 2026. There are hundreds, if not thousands, of companies offering cybersecurity services, presenting many different directions for companies to consider when creating a plan. It is therefore critical that businesses are allocating resources correctly and developing a strategic and actionable plan, lest they risk overspending without receiving the required protection.

This requires four key items:

1. Assess the scope of critical data
2. Identify the actual risks to that data
3. Allocate available funds by prioritizing the level of defense required for each risk
4. Create a cybersecurity defense plan and run a fire drill so all key actors are aware of the steps required during a real attack

https://www.mordorintelligence.com/industry-reports/cybersecurity-market

The intention of this cybersecurity white paper is to help executives and board members understand this process by answering the following questions:

- What does cybersecurity actually mean?
- How do you create a strategic plan?
- What is "cyber insurance"—and is it worth it?
- How can the right approach help executives sleep better at night?

The real-world definition of cybersecurity

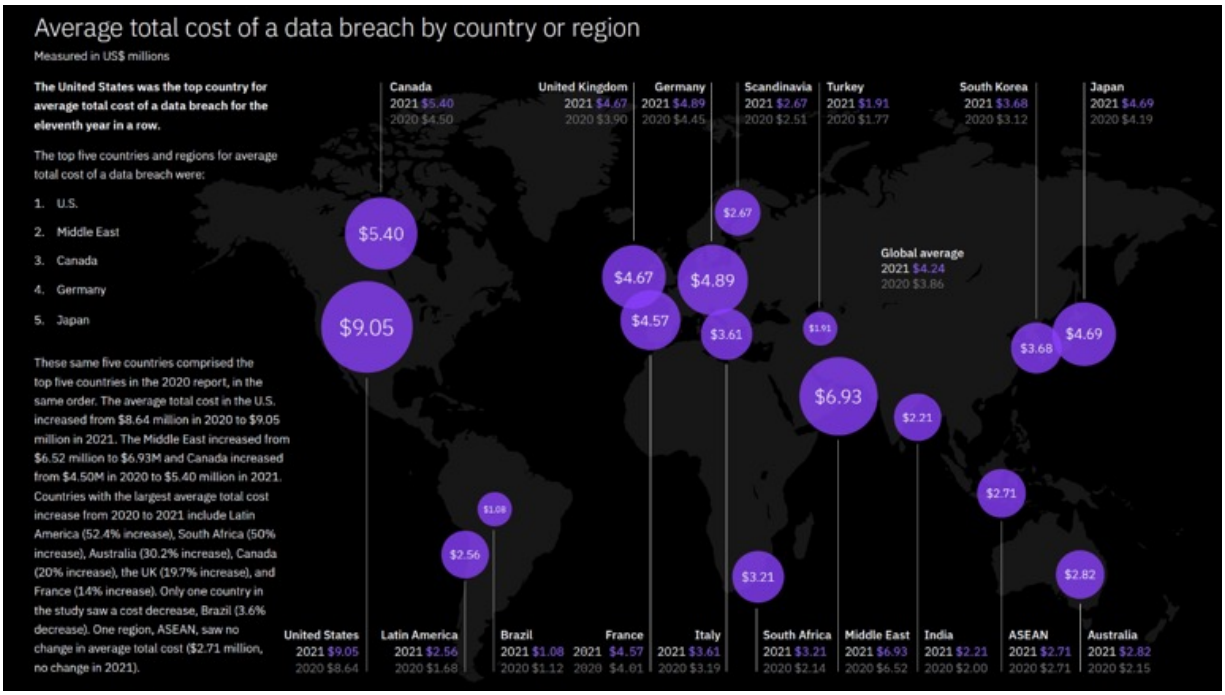
At its highest level, cybersecurity is the protection of critical infrastructure, data, and information from cyber attacks. Cybersecurity can be divided into several categories:

- **Network security:** securing a computer network from intruders
- **Application security:** defending against threats to devices or software
- **Information security:** protecting the integrity and privacy of the data that the organization collects, including its own data and its customer data
- **Operational security:** safeguarding the ability to access the data, including username and passwords and key positions
- **Disaster recovery and business continuity:** planning how to respond in the event of a cybersecurity incident
- **Physical security:** protecting physical servers, including the building that houses them, from both criminal (e.g., sabotage, theft) and environmental threats (e.g., excessive heat, flooding, earthquakes)
- **End-user education:** educating personnel on how to follow security measures to protect the organization

The Tremendous Cost of a Data Breach

The average cost of a data breach varies per country, with the United States leading the way with over $9 million per incident.

https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security
https://www.retarus.com/blog/en/data-breaches-costlier-than-ever-for-companies/



The highest cost of a data breach comes in the healthcare sector, followed by financial and pharmaceuticals. Health data carries additional costs because of significant government regulations governing the data, the impact to patients if the data is released, and the loss of historical records in the event the data cannot be recovered. Unfortunately, these are also areas that have less funds to focus on data protection and are frequently known as “soft targets”.

Building a strategic plan through comprehensive risk analysis

Measuring Risk

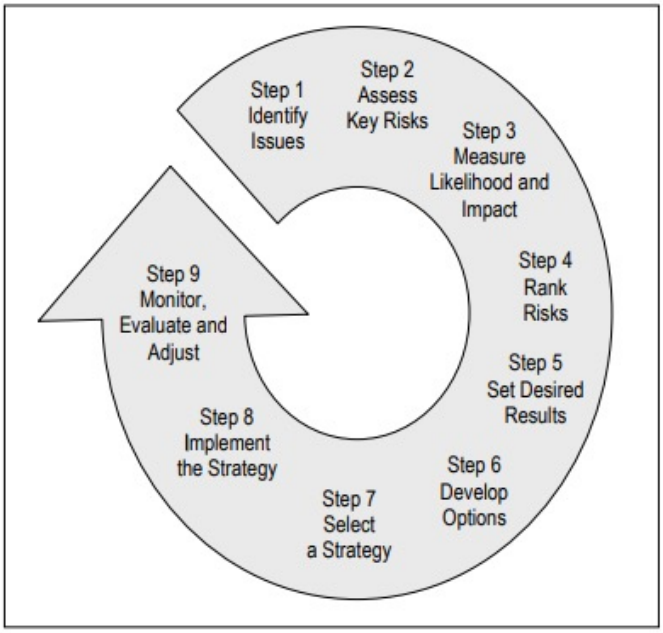
There are two primary types of risk measurement.

Quantitative risk measurement is a way to assign a dollar value to risk by calculating the probability of a given risk occurring and predicting the cost of mitigation.

Qualitative risk measurement is a “gut check”—a way to assess the potential risks associated with your data infrastructure and the potential disruption that an attack could cause. Both types need to be considered.

A common model used to assess risk is the Harmonized Threat and Risk Assessment (“HTRA”) tool. These are a set of tools used to address the risk to employees, assets and services. The model pictorially shows a 9 point process to measure and assess security risks:

https://cyber.gc.ca/sites/default/files/publications/tra-emr-1-e.pdf



Using this model, every aspect of the IT infrastructure can be evaluated and assigned a level of risk.

Each potential risk should be looked at from three angles:

- The likelihood that the risk will occur
- The financial and operational harm to the business if the risk did occur
- What level(s) of effective safeguards currently exist, and areas where new safeguards must be established

Cybersecurity Auditing

Identifying the risks associated with both a small and large business is not an easy task. This is because there are so many aspects of the organization that fit into each category. When we look at our organization, we often have biases and blind spots that cause an over- or under-estimation of the risk—or even render us totally oblivious to a major weak point.

That proximity-blindness is exactly why a cybersecurity audit is so critical. A sound cybersecurity audit should be a systematic, independent, comprehensive review and analysis of the business's IT infrastructure, including the various touchpoints. The audit should test and apply stresses to the infrastructure to identify the threats, vulnerabilities, high-risk practices and potential attack vectors. Finally, the audit should evaluate whether the policies and procedures in place would adequately protect the infrastructure from attack.

Cyber-Defense

Attackers continue to evolve and increase the sophistication of their methods, which fit one of four molds:

- **Opportunistic**

  These hackers tend to be less sophisticated. They look for a vulnerability that they can exploit and attack it.

- **Hacking Community**

  These hackers tend to be more sophisticated and will generally target specific organizations either politically or financially.

- **Organized Crime and Terrorist Groups**

  These hackers are also sophisticated with evolving capabilities that are designed to wreak havoc on a high-value target.

- **State-Sponsored**

  Government espionage targeting critical infrastructure and services of an opposing nation.

Unfortunately, cyber defense is always slower to evolve than cyber attacks. As a result, defense mechanisms need to be proactively monitored and upgraded, which is why a cybersecurity risk audit must be performed regularly (every year or every other year, depending on the industry) to ensure there is no false sense of security that could lead to a devastating breach.

Optimizing the allocation of cybersecurity funds

There is a proverbial saying, “Don’t kill a fly with a sledgehammer”. Companies have limited budgets and therefore must tailor their cybersecurity action plan to the appropriate risks. The greater the defense, the higher the cost and the greater the inconvenience or disruption to the business. Therefore, the task of the executives and board members is to find the optimal plan that prioritizes investment across all defense mechanisms, including on people education while also supplementing with a strong action plan and cybersecurity insurance.

Cybersecurity insurance is expensive and coverage is often limited. Insurance should not be relied upon as the primary defense but used as one component of the overall cybersecurity plan.

Establishing a strong cybersecurity plan

Start with low hanging fruit.
Build a corporate culture of cybersecurity awareness. When all employees are actively part of defending against cyberattacks, the risk to the company decreases.

Harmonize the cybersecurity strategy plan with the business strategy.
If the corporation is focused on critical data (such as health data), greater allocation to protecting third party data is required. Corporations should map to the intelligence gleaned from the cybersecurity audit very carefully.

Practice for an attack.
Ensure that there is an adequate response plan—and practice the plan so there are no surprises.

Cushion against critical losses.
Consider cybersecurity insurance to protect your company from any potential loss should an attack be successful and systems are shut down.

Sleep better.
Finding the right balance between defense, education and insurance will leave the company in a good position—and allow executives to sleep better at night.