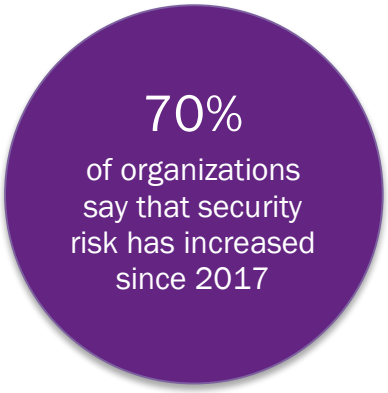
The Strategic Importance of Cybersecurity

By: Connor Jackett and Narek Sarkisyan August 2018

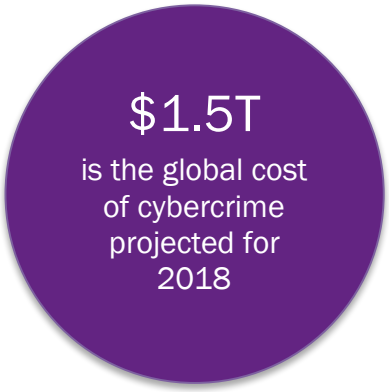
"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it"

– Stephane Nappo, Global Chief Security Officer at Societe Generale

Modern-day criminals are different from a Bonnie and Clyde duo wearing ski masks and pointing a gun at a bank teller. These new criminals hide behind the safety of a computer, hacking the most secure and protected networks looking for personal, corporate, and private information.



1



2

In the first half of 2018, global business icons such as Facebook, Walmart, FedEx, and even trusted financial institutions, such as CIBC[3], were breached. The hacks leaked customers' personal information on black market websites. Each cyber-attack costs corporations millions of dollars, while also tarnishing their reputation in their respective industries. In the case of CIBC, a cyberattack affected 90,000 customers by hackers freezing accounts, committing financial fraud, and stealing personal information. CIBC now faces countless lawsuits and a complete revamp of their cybersecurity system resulting in large fines and an increase in security costs.

Equifax Breach in Snapshot

In 2017, Equifax's nightmare became reality. In a matter of minutes, 147 million customers were affected by a security breach that exposed social security numbers, addresses, credit card numbers, Tax ID numbers, and many other personal forms of information.

Today, they are still cleaning up this mess. To date, Equifax has spent US$243 million on improved IT and data security, legal and investigative fees pertaining to the breach, and hiring additional security and IT staff. Along with the millions spent on restoring their company reputation, an executive was charged with insider trading after knowledge of the breach was released to employees.

Equifax is continued to be mentioned in the news in conjunction with cyber-attacks and financial issues regarding their reorganization.

There is a growing concern among organizations about potential breaches in their systems as well as users demanding transparency in how these organizations handle their data. Such concerns are also being voiced in boardrooms given that cybersecurity oversight is becoming an important responsibility for board members. Boards' increasing involvement in

[1] https://blog.barkly.com/2018-cybersecurity-statistics

[2] https://securityintelligence.com/20-eye-opening-cybercrime-statistics/

[3] Canadian Imperial Bank of Commerce

cybersecurity matters is not only due to its enterprise-wide risk but also due to its major strategic implications such as operational planning, capital expenditure decisions, and internal processes and policies.

Cybersecurity as a Strategic Decision

Restricted Growth	A data-breach comes at a high cost usually ranging in the millions of dollars. Lack of sufficient security, therefore, puts a company at risk of restricting growth as well as hindering opportunities to expand.
Tarnished Reputation	Due to an attack, the reputation of a company can become permanently tarnished, resulting in lost trust as well as decreasing performance.
Regulatory Actions	Along with rising costs and lost trust, companies also must deal with a variety of legal actions that take time and resources away from the business.

The underlying implications of an attack affect growth, reputation and general business strategy within a company. After an attack, the focus of an organization can shift from meeting strategic objectives and adding value to stakeholders to saving reputation and cost cutting to repair the damages. The implementation of cybersecurity measures becomes an important strategic decision involving detailed assessment of resource allocation, review and selection of appropriate tools and systems, and analysis of similar use cases in the industry.

Strategy

Selection

Selecting the right cybersecurity approach is critical in mitigating risk and decreasing vulnerability. Purchasing the most innovative and elite cybersecurity system is not always the best option given a company's financial situation and what information they are protecting. The decision starts by understanding the needs of the company and the cyber risks they are facing. For example, a large financial institution, that not only holds private information (such as addresses and telephone numbers), but Social Insurance Numbers and access to people's money, requires more security than a firm that only holds a user's email and phone number on file.

Implementation

The implementation of the security system is also important in the process of creating a strategy for securing data. Implementing cybersecurity technology correctly and successfully is essential and the complexity of this task is often underestimated. It is essential to know what IT systems are in place and how they are connected to the organization's network.

Monitoring

Making sure that the technology is performing the way it should and ensuring there are no gaping holes in the network is the final step in creating a strategic cyber defense system. Hiring more IT and cybersecurity analysts to monitor the system can lead to better effectiveness of the security system.

Innovative Cyber-Defense Technologies

In the rapidly changing world of technology, two major additions have greatly impacted the cybersecurity industry. AI and Blockchain technologies can be used in a variety of ways to better secure data and personal information. These new technologies have also changed how certain companies are shifting their strategic approach to keeping their data secure.

AI: Machine Learning and Predictive Analytics

AI combined with machine learning and predictive analytics is revolutionizing the cybersecurity industry. With the inclusion of AI, corporations can mitigate risk by using the technology to recognize when a cyberattack will happen. AI can also help prevent attacks by finding new exploits and weaknesses that can be quickly identified before an attack. The most innovative feature of AI is the ability to learn and improve as each threat is analyzed by the machine. The possibilities are endless as the technology learns from every system it analyzes and develops a strategy for solving future threats.

LogRhythm, a developer for cloud-based AI technology, is a pioneer in the cybersecurity industry. They are using AI and advanced machine learning algorithms for security that accelerate threat detection, maximize analyst efficiency, and evolve completely on its own. As more companies adopt AI solutions into their security systems, problems of cyber breaches and lost customer data will diminish.

Blockchain: Decentralized Security

Blockchain is radically improving the cybersecurity industry in three main ways: decentralized storage, authentication, and traceability. The decentralized system spreads each set of data across a system of networks making it impossible for a hacker to easily break into one central system that contains all of the data. Blockchain technology also eliminates the need for human factor identification (email/password login), which takes away a potential entry point for a cybercriminal. Finally, Blockchain enables a company to track every transaction with a digitally signed time stamp. The traceability function of the technology allows for corporations to pinpoint where, when, and how the attack occurred leading to security improvements and more advanced attacker identification. Blockchain enables security systems to decrease the amount of threats, while also enabling companies to identify an attacker if a breach occurs.

Altr, an innovative cybersecurity company, recently announced that they are developing a blockchain-powered data security system. The security platform will “restore digital trust by transforming the way your data is monitored, accessed, and stored”. The system includes increased visibility and transparency, efficient fragmentation of the data, and automated real-time breach prevention.

Board Oversight

Although technological developments are greatly impacting the cybersecurity industry, the problem is not solved. As security develops, so do the attackers. The evolutionary technological race between hackers and cybersecurity firms will go on forever. Even Blockchain security systems, such as the one used for Bitcoin, have been hacked, which resulted in millions of dollars being lost. Corporations, institutions, governments and users are all constantly at risk of being exposed. The many financial and reputational risks that come from a cyber threat make investing in a security system a strategic decision that involves a great deal of thought, from the selection of a security system to its alignment with the organizational infrastructure and business needs.

Cybersecurity is a complex and rapidly evolving subject which is why cyber expertise at the board level is uncommon. Nonetheless, one of the board's key responsibilities is to challenge management on key opportunities and risks facing an organization. That is why it is vital for directors to establish effective mechanisms that support a healthy board-management dialogue on cybersecurity. Constantly challenging and asking questions about the existing cybersecurity technology as well as effectively monitoring its progress will lead to better decisions and a more secure network. The following questions can help start the conversation and ensure this topic is well covered on the boardroom agenda:

- ? What framework does management use in designing its security program and how effective is it?
- ? How are we assessing business needs against security risks when making technology investments?
- ? How does the organization's security program and infrastructure compare to that of its peers?

The Black Box Institute is a boutique advisory firm and think tank that provides purposeful and thoughtful guidance to clients. We specialize in complex business, transactional and organizational challenges. Our problem solving techniques incorporate a blend of traditional strategy and financial advisory capabilities with creative design thinking.

The Black Box Institute

For more information, please contact:

Janet McLeod
200 King Street West, Suite 1301
Toronto, Ontario, Canada
T: 416.862.5487
F: 416.861.9268

www.theblackboxinstitute.com
/the-black-box-institute