Secureworks®

WHITE PAPER

The Risk of Not Futureproofing Your Cybersecurity

Failure to Plan for the Future Can Put Your Whole Company at Risk

In Delphi, inscribed on the walls above the entrance to the Temple of Apollo were the words "Know Thyself." This maxim is extremely relevant as many organizations are challenged by the idea of futureproofing their networks, systems, hardware, software, and educating their employees against potential cybersecurity threats.

Knowing thyself (or thy company) is paramount in creating a comprehensive plan that not only focuses on the corporate assets, data, or information but takes into consideration all parts of the organization.

$1B+

yearly investment in cybersecurity by Microsoft.

$15B

budget allocated for the U.S. President's spending on cybersecurity.

Where the Challenges Reside

Business moves fast. Most organizations are consumed with the daily management of operations, driving resources to achieve quarterly earnings, or pushing against the schedule to get their latest products and services to market ahead of the competition. It's no wonder business leaders lose sight of the importance of preventing potential threats. Oftentimes, it's not until an organization has encountered a breach that they realize they should have invested the time to futureproof their cybersecurity strategy.

Business leaders are challenged with where they should invest within the organization. So how much money is enough to allocate for security? Unfortunately, there is no one-size-fits-all answer. The budget ranges per organization or industry. Microsoft revealed they will invest more than $1 billion each year in cybersecurity for the foreseeable future[1] and the U.S. President's budget allocated $15 billion in spending on cybersecurity.[2] But don't fall into the trap of thinking money alone can solve your security challenges; non-monetary factors like culture and leadership also play into the formula.

Many organizations shy away from implementing a futureproofing strategy. This is due to the lack of personnel or technical resources to help manage and monitor security programs, and sometimes security leadership is ill-equipped to provide direction. In many organizations, security staff are overworked. Some simply do not have the bandwidth to take on more projects.

What Exactly is Futureproofing?

Futureproofing is essentially the practice of implementing a strong risk management strategy. It requires a forward-looking assessment of your risk to inform security decisions that prepare you for the future. Of course, there is no way to completely futureproof everything. In security, the unexpected can happen. Organizations should build flexibility into any security program so they can remain nimble under all circumstances. That means continually assessing the foundations of your security program and accounting for any potential weaknesses.

[1] Reuters, Microsoft to continue to invest over $1 billion a year on cyber security

[2] Whitehouse.gov, Cybersecurity Funding

Security teams should assemble twice a year to assess the threat landscape and to determine what they'll need in the future to maintain security. Futureproofing planning should involve:

- Identifying all types of company data, such as personal financial information, intellectual property, customer records, and any classified information. Defining where that information is stored, such as databases, spreadsheets, text documents, or file shares. Consider how company handling of data is likely to change in the next 12-24 months and the implications for security.
- Performing an audit of all hardware, software, and devices within the network to understand what devices are used, such as mobile devices, laptops, or tablets. Understand the tools you use so that you can identify potential problems and areas that may prevent you from achieving future goals.
- Understanding how the threat landscape is changing and where it is likely headed. Are there strategies and tactics you can employ that will keep you protected even if predictions fail and the threat landscape evolves in unexpected ways?
- Discussing if a third-party vendor can offer the threat intelligence and peer insight you need to thoroughly assess risk and build a robust plan for the future.

The only way to successfully mitigate the risk these changes create is by identifying where they are headed in the coming months and working cross-functionally with other business leaders to build a holistic strategy.

What Constitutes the Future?

Security evolves so quickly it doesn't always pay to plan too far out. Given the changes in the world, both from a business and social standpoint, organizations should realistically be looking at six to 12 months, and no more than two years out, especially with the threat landscape changing at a rapid rate. Likewise, everyone within the organization who is involved in the planning should sit down quarterly and review to make adjustments, spot industry trends, and reassess their forecast accordingly.

Collaborate Internally, Look Externally

Organizations are navigating rapid change and complex infrastructures with significant implications for business leaders. The only way to successfully mitigate the risk these changes create is by identifying where they are headed in the coming months and working cross-functionally with other business leaders to build a holistic strategy. This process should also involve analyzing what your peers are doing to see what steps they're taking to stay protected. There's a lot to learn from assessing what similar organizations are getting right, and what they're doing wrong. Partnership with an experienced vendor can often provide insight and best practices from industry peers that you may otherwise not have access to.

The Challenge Futureproofing Poses

Leadership and the planning team have to understand the potential risks involved in securing the information and data they possess, and how those risks will change over time. Discussions must take place around what happens if that data is breached, what it could potentially cost the company, how it can impact the brand, and the ramifications to the customer if it lands in the wrong hands. Serious consideration should be given to how PR and marketing will shape public perception so the brand image of the organization is not tarnished.

Emerging technologies should play a role in any plan. Artificial intelligence and machine learning can offer impressive productivity gains and address blind spots for security teams, but learning to see through the hype to understand what really works takes time. Other business technology developments like cloud computing, increased mobile device use, and the Internet of Things should be considered, especially as they can expand the attack surface for threat actors. It's important to understand how the process of adopting these technologies will change your risk profile over time.

Organizations should remember that threats or bad actors not only reside on the outside of organizations, but the inside too. Too many companies spend great time and effort securing their organization from outside threats, only to be taken by surprise from the inside.

$3.92M

average cost of a data breach.

$150

cost per record in an average security breach.

Assessing the Risks — What are They?

In terms of risks, business leaders – along with their legal department – should take the time to review their cyber insurance policies. The cyber insurance industry right now can seem uncertain and not well regulated. There are many cases currently in litigation where it's not totally clear who or which company was at fault.

Many organizations are also under the impression that they are fully covered, but they may not truly understand what they are covered against. Consequently, they'll need to safeguard against any loopholes. It's also important that the legal team is involved in every step of the process.

What's at Risk if You Don't Futureproof?

Failure to plan for the future puts your whole company at risk. A breach can tarnish your reputation, compromise your data, affect your profits, cripple your systems, and lock out your workforce. And in extreme cases, it can be a life or death situation – especially in healthcare breaches where ransomware is involved.[3]

[3] Business Insider, Hospital cyberattacks linked to heart attack deaths, study shows

Secureworks®

Recent research indicates that the average cost of a data breach is $3.92 million.[4] The average breach costs an organization $150 per record, which might not sound like a lot until you do the math. (If you have 100 records it can cost $15K. If you have 10,000 records, it can be $1.5 million.)

In our current threat landscape, it's imperative that organizations futureproof. With a proactive plan that accounts for future trends and uncertainty, business and security IT leaders are equipped to handle and recover from an attack faster with better response and efficiency.

Benefits of Cyber Literacy

Many organizations have implemented some form of cybersecurity education program – whether it's classroom instruction, online tutorials, or quarterly review updates. Studies show many breaches and data exposures come from human error or intentional misconduct.[5]

An educated workforce can help stop the spread of a breach through an ability to recognize a phishing email or smishing text. Educating employees on the threats they could face can avoid the need for expenditure on incident response later.

What Areas are Organizations Overlooking?

With an evolving work culture allowing many employees to work remotely, coupled with the COVID-19 pandemic that accelerated the trend, organizations are forced to consider the new risks that follow.

A hasty work transition can create challenges for organizations that have no protocols in place to account for the security implications. Research showed a spike in phishing emails using the coronavirus to trick individuals into clicking links or downloading attachments that included viruses such as ransomware.[6]

Part of reviewing and developing a comprehensive futureproofing plan should include how the organization's profile has changed over time and how it might change in the future due to business growth, economic changes, or other factors.

Communication is Essential to Any Plan

When it comes to planning for a potential breach, marketing and public relations are critical – yet often overlooked. When a breach occurs, the organization goes into crisis management mode and timing is everything. This is the time when cross-functional team input pays off as executives from IT, security leaders, and directors within the business units carry out their assigned roles.

Part of reviewing and developing a comprehensive futureproofing plan should include how the organization's profile has changed over time and how it might change in the future due to business growth, economic changes, or other factors.

[4] IBM Security/Ponemon Institute, 2019 Cost of a Data Breach Report

[5] Infosecurity Magazine, Human Error Linked to 60% of Security Breaches

[6] The Hill, Cyber threats spike during coronavirus pandemic

Excluding marketing and PR from your futureproofing initiatives can ultimately place the brand's reputation at stake. Think back to the Wells Fargo Bank breach a few years ago where employees were opening fake accounts. Not only did it hurt the bank's reputation, but it resulted in record fines, the removal of key executives, and a drop in stock prices.[7]

Before the situation unraveled over several weeks, it was the bank's legal and PR departments that stepped up and issued statements to address the situation.

When a breach occurs, one of the worst things a company can do is try to manipulate the facts. Successful organizations are transparent about what they know, when they know it, and the steps they are taking to remedy the situation.

Observing what peers are doing and what trade groups recommend is key to a successful plan. A futureproofing strategy encompasses everyone, so the entire corporate culture has a sense of the importance security plays.

Keeping Your Futureproofing Proactive Instead of Superannuated

The value of futureproofing lies in having a robust, living framework that can be constantly evaluated, tested, and reviewed by experts within and outside of your organization.

That value is created by gathering differing points of view from cross-functional teams, business units like risk management, legal, marketing, and PR – along with the ongoing solicited feedback from peers and industry experts. Focusing only on what you're doing internally can prevent you from learning about the best practices and strategies that others are using. Observing what peers are doing and what trade groups recommend is key to a successful plan. A futureproofing strategy encompasses everyone, so the entire corporate culture has a sense of the importance security plays.

To truly build a holistic view of your organization's cybersecurity vulnerabilities, it comes back to knowing thyself. Knowing the who, what, where, when, why, and how can help ease the challenges associated with futureproofing.

Creating a comprehensive plan not only involves looking backward, but also looking forward, proactively. Your plan should take into consideration all the moving parts and the connecting pieces that define your products/services, and brand image of who you are in your industry. Futureproofing is vital to your organization's security.

[7] CNN, US government fines Wells Fargo $3 billion for its 'staggering' fake-accounts scandal

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp