WSJ PRO CYBERSECURITY

ESI THOUGHTLAB

THE CYBERSECURITY IMPERATIVE

EXECUTIVE SUMMARY

PROJECT SPONSORS

hp CyberCube Baker McKenzie. KnowBe4 Human error. Conquered. protiviti Face the Future with Confidence Willis Towers Watson opus SIA Security Industry Association

Introduction

Cyber risk has become one of the top challenges for any business to deal with. A single cybersecurity incident can significantly disrupt operations, result in loss of revenues leading to longer term financial damage, bring regulatory and legal actions and damage an organization's reputation and the confidence of its customers. The majority of businesses understand that cybersecurity cannot be left to the information technology team to deal with alone.

Internal knowledge of the organization's cybersecurity strategy at the senior executive and board level is improving. It is critical that leadership teams and boards have a clear view of how the company is addressing cyber risk and to understand how data loss incidents could harm the business. In turn, this drive towards visibility and stakeholder awareness has helped promote cyber risk management in the enterprise.

While the situation may be improving internally, *limited knowledge sharing externally is hindering widespread improvements.* Threat information sharing is relatively common between the public and private sectors and among organizations within the same industry vertical, but the same is not true for sharing information around how organizations are tackling cyber risk challenges, prioritizations and investments in people and technology.

A lack of visibility across industries hinders not only the benchmarking of preparedness and programs, but also cybersecurity investment decision-making. Moving from a security program that is compliance-focused, to one that aligns to risk management best practices, through to a mature program of continuous monitoring and improvement of security processes that emphasizes resilience requires not only a long-term commitment and resources, but also on business leaders that are motivated to invest.

The 2018 WSJ Pro Cybersecurity Benchmarking study aims to provide such motivation. For the first time, an independent research company, ESI Thoughtlab, has collected data from over 1,300 companies worldwide to allow for thorough benchmarking in a range of cybersecurity-related areas. More information on the companies in the study is provided in the Research Background section of this report. The data was collected during the second quarter of 2018, primarily from companies operating in the financial services, manufacturing, energy/utilities, consumer markets, and technology. Answers were provided by senior executives and a number of in-person interviews were conducted with business leaders and subject-matter experts to collect more detail and insight.

The research revealed one crucial finding: managing cyber risk effectively requires organizations to invest in and improve their cybersecurity strategies continually; the success of this endeavor requires the support from senior executives who set the tone at the top.

The purpose of this report is to summarize key findings and draw lessons learned to provide senior executives with decision-making support to enhance their cyber risk management strategies.

In analyzing the results of the survey, the report will focus on a number of areas in greater depth:

- How organizations are performing in relation to the NIST Cybersecurity Framework
- The economics of cybersecurity and where organizations are spending their resources
- The perception of cybersecurity threats and risks
- The governance of cybersecurity

This summary report includes a number of 'calls to action' extracted from the results and from the insights of individual contributors.

Key Findings

This is a first-of-its-kind study and produced a wealth of valuable data about how companies across multiple geographies and industries are approaching cybersecurity. A greater depth of insight and interpretation can be found in the full report. Here are a few of the key findings:

• 100% of respondents, all business or technology leaders, claimed to be well-informed about cybersecurity policies, systems, and practices.

• Perceptions of cybersecurity change as a company's approach matures: 19% companies assessed as 'beginners' on the cybersecurity journey see cybersecurity as a reputational risk, in contrast to 41% of 'leaders'. 23% of leaders saw cybersecurity an area of competitive advantage compared to 6% of beginners.

• 70% of all companies surveyed view cybersecurity as a financial risk, 62% view it as a technology or IT risk, and only 55% of organizations view it as an operational risk.

• For technology companies, 73% see cybersecurity predominantly as an IT/technology risk, the highest of any group. 87% of insurance companies see cybersecurity as a financial risk, the highest of any group.

• The rise of new technologies, such as artificial intelligence, Internet of Things and blockchain, and the use of open platforms are seen as having the greatest impact on cyber risk. Our study identified a correlation between the digital maturity of a business and their cyber risk exposure.

• *Unsophisticated hackers (59%) and cybercriminals (57%) are seen as the greatest external threats, while state-sponsored attackers were a concern for only 3%.*

• *87% of companies believe untrained general staff represented the greatest cyber risk within their organization.*

• Third-party cyber risk is a growing area of concern. While only 1 in 5 businesses are currently concerned about the likelihood of being attacked through customers, partners and vendors, that number rises to 70% who see the same as a risk they will have to deal with in the next two years, an increase of 247%.

Calls to Action

Through the data collected in our study and the subsequent analysis and supporting interviews, we have identified a number of key focus areas that can help reduce risk and potential impact for all businesses, regardless of size, geography or industry vertical.

1. Getting The Basics Right

The challenge of securing data, networks and users is significant, but before an organization seeks to tackle some of the more complex problems, it must first ensure the fundamentals are in place and that processes to execute on the fundamentals are robust. These measures are often referred to as 'cybersecurity run-in'.

Run-in measures are not officially defined, but generally encompass a range of core security controls.

For instance:

• Understand the design of the network and what needs to be secured. Maintain an inventory of devices that connect to the network and a whitelist of software allowed to run on machines.

• Applying security updates is a priority. Reducing the window of opportunity for weaknesses to be exploited by cybercriminals is critical. Almost 13,000 software vulnerabilities have been published in the first nine months of 2018, more than at the same point in any previous year, and exploits are typically available several days before the average organization closes the security hole.

• User awareness is a large part of cybersecurity hygiene and is broken out below as a separate point, such is its importance.

• Secure machines and data with encryption to mitigate the risk of data loss either as a result of an attack or the loss or theft of a corporate device.

2. Ongoing Cybersecurity Awareness

Our survey found an overwhelming majority of respondents viewed untrained employees as the greatest cyber risk to their businesses. This is not to say that users, untrained or otherwise, are stupid, negligent,

careless or reckless, it is simply to say that criminals and attackers use this vector of attack the most. Attackers socially engineer victims to click on links or to open attachments that will result in their machines becoming infected. Sophisticated attackers meticulously research their victims in order to create the most authentic looking emails, which their victims will most likely interact with.

Most organizations brief new hires on cybersecurity during their onboarding. However, far too often, this is the first and only time cybersecurity is mentioned, and usually is communicated as part of a large volume of information new hires receive. Thus the message may not be received as one of crticial importance to the organization. Cybersecurity is a dynamic subject and employees must be regularly briefed on the latest tactics employed by cybercriminals. Building a distrust of the unfamiliar and learning the warning signs of a phishing email take time. Security professionals often forget this.

According to a recent survey[1], only 5% of organizations run a mature cybersecurity awareness program. Programs take time to build, must be supported by senior executives and have full-time resource allocated to them. Communications skills should be valued over security skills–employees will only learn if the content is engaging and relevant. Finally, the training must be ongoing and tailored to individual needs with regular updates if a change in culture is to be achieved.
Many organizations choose to conduct phishing attacks against their staff to better understand how effective cybersecurity awareness training has been for staff and to identify individual employees that may be more susceptible to phishing in order to target remedial training.

Any individual can be duped into opening a well-crafted phishing email, but organizations must ensure their employees are able to identify suspicious emails most of the time and, in the event a mistake is made, the employee knows how to report the incident and can do so without fear of recrimination.

3. Baking Security In, Not Bolting Security On

Digital transformation has fundamentally changed the way businesses engage their customers and run their businesses. Security is at the heart of that transformation. In an age when applications are created and updated more frequently than ever before, it is essential that security is an integral part of the development process.

Where security is an afterthought, the release of the application could be delayed and revenues could be lost.

1. See pge 30 of 2018-SANS-Security-Awareness-Report

However, the release of an insecure application could result in a massive loss of user trust and expensive post-release fixes that could negatively impact the whole organization. Security and privacy must be included 'by design' to help build customer trust.

The security team must be included on business decisions at the earliest point possible, sharing their knowledge of security with both the leadership team as well as developers. The importance of this exchange increases when a business is digitally mature.

The CEO must ensure security is part of the discussion by engaging the CIO, CISO and CTO, and in some businesses, the Chief Privacy Officer. Through their collaboration and shared accountability businesses can get products to market or make internal technology advancements without security slowing the process or becoming the cause of expected costs later.

4. Resilience Through Exercises

Resiliency allows an organization to expand and contract, rather than break. Broadly defined, resilience is the ability of any company to return to normal operations following a period of upheaval. That could include anything from a natural disaster to accounting fraud, but cybersecurity brings financial, commercial, legal, compliance, and reputational risks for any business in addition to the potential for large-scale operational disruption.

Too few enterprises have dedicated the proper focus to ensuring that they're able to withstand incidents like prolonged downtime or ransomware intrusions. This lack of preparation leaves companies dangerously exposed to severe operational impact in the case of a cybersecurity incident.

Organizations must prepare for cyberattacks and business disruption by conducting drills at both the working and senior executive levels.

At the working level, security teams need to refine their incident response plans and have playbooks for detecting, investigating and remediating threats before real damage occurs. For example, the likelihood of being hit by a ransomware attack is high for all businesses and therefore understanding how to quickly isolate the affected machine from the network and restore backup data to both minimize disruption and avoid having to pay a ransom is essential.

At the senior level, the discussions and the plans that need to be put in place are different. Bringing senior decision-makers together to get familiar with the types of incident that could affect the company is paramount to understanding the risks they bring. A CEO must confide not only that the technical response is adequate,

but also that the company will have access to the best legal and communications expertise to help manage fallout from the incident and sufficient insurance to cover post-breach expense–for example, the costs associated with notifying customers of a breach.

Preparedness for breaches is especially important for small and midsize companies that do not have the same access to expertise and may be disproportionately affected by a cyber incident. The ability to swiftly respond to an attack and mitigate damage may be the difference between minor disruption and going out of business.

5. Board-Level Engagement

No one expects the average board member to have an in-depth understanding of the technical nuances of cybersecurity or the complexity of securing software, but nor is it necessary. What is important, however, is the ability to grasp the significance of cyber risk and the potential for serious business impact, and a firm comprehension of the risk management strategies required to deal with those risks. After all, cyber is simply one more business risk, albeit with significant consequences if it is not managed effectively.

Businesses that carry particularly high levels of cyber risk, especially those operating in sectors where cybersecurity defenses are often tested by sophisticated attackers, will want to consider recruiting a board member or external advisor with cyber expertise. This provides an enhanced level of knowledge on the board and clearly demonstrates the company is making cybersecurity and cyber risk mitigation a priority.

Boards must be given a clear picture of their business's preparedness to detect and respond to attacks, an appreciation of the data or assets that could be targeted and the potential impact of a successful attack. Additionally, boards should see metrics related to the ongoing improvements in risk identification and management and an assessment of whether the skills available in-house are sufficient to maintain security and progress a cybersecurity strategy. Boards need to also consider risks from beyond the company's perimeter: What is being done to ensure suppliers and other third parties are not creating additional risk for the business through their poor security practices?

A board's continued interest in and support of the cybersecurity strategy will encourage those working hard to secure the organization. Boards will dictate the frequency of updates, but many large enterprises have cyber risk briefings as a standing agenda item.

6. Investment with Impact

Our survey highlights how companies are investing in cybersecurity and the continued increase in investment is encouraging, but staying one step ahead of the criminals doesn't come cheaply. As we set out above, hygiene measures do not have to be hugely expensive, but an organization cannot defend itself with hygiene controls alone.

As businesses large and small consider where to spend their information technology budgets, ensuring the money is spent wisely is critical. Money wasted on the wrong service or product, or money spent mitigating the wrong risks could result in security breaches that cost the organization dearly.

Buying the latest technology solutions alone is not the answer without the skilled individuals able to drive the solutions and derive value from them. By the same token, recruiting skilled talent without the tools required to allow them to find anomalous or malicious activity on the network may also leads to failure. Too much investment in trying to prevent attacks might be at the expense of responding to the inevitable while the opposite is also true–not enough spent on prevention could lead to over-utilization of the response team because even low-level attacks are successful

Choosing the right cybersecurity vendor is not straightforward: hundreds of vendors compete with thousands of products. Opting for a single vendor with a portfolio of products may result in a compromise on quality, opting for multiple vendors with best-of-breed products may result in solutions that do not interact easily with one another. Neither situation is ideal.

The key to success is a well-constructed cybersecurity strategy with clear priorities. Spending must be balanced between people and technology with careful consideration for which risks should be addressed in which order. Decision-makers must be mindful of how their choices map against the NIST Cybersecurity Framework to deliver a rounded set of defenses.

Research Background

To carry out our cybersecurity thought leadership program, we used a rigorous, mixed-methods research approach consisting of four elements:

1. Cross-industry survey of 1,300 executives worldwide with insights into their companies' cybersecurity approaches and results.
2. Consultation with an advisory board of experts and practitioners from leading organizations with varied perspectives on cybersecurity.
3. In-depth interviews with CISOs and other executives across industries, as well as with selected cybersecurity experts.
4. Return-On-Investment and cost-benefit analysis to assess and benchmark the impact of cybersecurity measures on corporate performance.

Our survey respondents included executives from organizations in all major world regions, spanning companies with under $1 billion in revenue to very large enterprises with over $50 billion in revenue. To ensure the breadth of our analysis, we also included public companies (70% of total), private companies (22%) and government-owned firms and NGOs (7%).

Responses were gathered from companies across the globe to produce a fair reflection on cybersecurity progress:

To understand how cybersecurity strategies and performance results vary by sector, we surveyed a cross-section of industries. Respondents consisted of C-level executives and their reports. Each was responsible for cybersecurity practices in their companies or had direct knowledge of these activities.

To manage this pioneering research project, we brought together a multidisciplinary team from both ESI ThoughtLab and WSJ Pro Cybersecurity. To give us the benefit of their experience and insights into cybersecurity issues, we assembled a distinguished panel of executives from a variety of companies, associations, and industries.

To assess the cybersecurity maturity of companies, our diagnostic survey asked executives to rate their progress in five functions prescribed by NIST and common to other frameworks: identify, protect, detect, respond, and recover.

Our economists calculated category scores based on a ranking of 0 to 4 for each underlying activity. We summed the scores for each category to determine a composite score for each company. We then aggregated the scores to show trends by industry, location, revenue size and other key parameters. We used these scores to segment respondents into maturity stages and to benchmark their performance.

Research Partners

ESI THOUGHTLAB

CyberCube

Baker McKenzie.

hp

KnowBe4
Human error. Conquered.

protiviti®
Face the Future with Confidence

Willis Towers Watson

opus

SIA
SECURITY INDUSTRY ASSOCIATION