ESI THOUGHTLAB

The Cybersecurity Imperative

Managing cyber risks in a world of rapid digital change

A briefing paper from ESI ThoughtLab

October 23, 2018

Sponsored by:

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

Background on the study

By 2021, cybercrime will cost the world $6 trillion annually according to Cybersecurity Ventures, more than the combined GDP of the UK and France. As firms embrace the latest digital solutions and respond to rising regulations, cybersecurity has become a top management priority across industries and markets.

Cybersecurity is a moving target: as companies adopt new technologies, so do hackers. The reluctance of firms to share cybersecurity information makes benchmarking more challenging. To fill this gap, ESI ThoughtLab joined with WSJ Pro Cybersecurity and a group of leading organizations to launch ***The Cybersecurity Imperative***, a rigorous global research program. Our sponsors included Baker McKenzie, CyberCube, HP, KnowB4, Opus, Protiviti, SIA, and Willis Towers Watson.

To identify cybersecurity best practices and performance metrics, we conducted four levels of analysis:

1. A diagnostic survey of 1,300 firms across industries and regions.
2. In-depth interviews with 18 CISOs and cybersecurity experts.
3. Insights from an advisory board of executives from sponsoring firms and DTCC, Evolver, Fidelity, Hubbard Decision Research, NIST, and Security Mantra.
4. An economic model benchmarking the impact of cybersecurity practices on performance.

As part of our analysis, we scored surveyed companies by their reported progress against each of the five pillars of the NIST framework: identify, protect, detect, respond, and recover. According to those rankings, we then segmented companies into three stages of cybersecurity maturity: **Beginners, Intermediates** and **Leaders**. We summed the scores to arrive at a firm's composite score for each category and overall and assessed the impact on their cybersecurity practices and performance.

Key findings and insights

Our extensive research of companies across countries and industries revealed 12 major cybersecurity findings. Senior management teams and cybersecurity experts will want to keep these trends and insights top of mind as they build systems to secure their digital future.

1. **As companies embrace new technologies, move to open platforms, and tap ecosystems of partners and suppliers, their cyber-risks will multiply.** While firms now report the biggest impacts from malware (81%), phishing (64%), and ransomware (63%), in two years, they expect massive growth in attacks through partners, customers, and vendors (247% growth), supply chains (+146%), denial of service (+144%), apps (+85%), and embedded systems (+84%).

2. **While firms see high risks from unsophisticated hackers (59%), cyber criminals (57%), and social engineers (44%), the greatest threat lies within: untrained general staff (87%).** Another 57% of firms see data sharing with partners and vendors as their main IT vulnerability. Nonetheless, only 17% of companies have made significant progress in training staff and partners on cybersecurity awareness—a clear weakness for many firms.
3. **When developing a cybersecurity roadmap, firms need to address the "digital paradox."** When digital transformation outpaces cybersecurity progress, companies bear a bigger chance of suffering a major cyber-attack (over $1m in losses). Digital leaders in early stages of cybersecurity have a 27% chance of having a major attack, compared with a 17% probability for digital leaders with advanced cybersecurity systems.
4. **Companies need to ensure their cybersecurity investments don't fall behind.** Our survey shows that firms increased their cybersecurity investments by 7% over the last year, and they plan a 14% boost next year. The biggest upsurge is coming from platform companies, which hiked their cybersecurity investment by 59% over the last year and plan a further 64% bump next year. On average, companies with revenue between $250m-$1bn will spend $2.9m next year, $1bn-$5bn ($5.7m), $5bn-$20bn ($10.7m), and $20bn+ ($16.8m).
5. **Cybersecurity investments will vary by industry, size and location next year.** Energy/utility firms plan to increase spending the most (21%) followed by consumer goods/services (+17%), technology (+16%), insurance (+14%), life sciences/healthcare (+12%), financial services (+11%), and manufacturing (+3%). The biggest hikes will come from smaller firms with $250m to $1b in revenue (+40%) and with $1b-$5b in revenue (+37%). Firms based in South Korea, facing government-sponsored risks, will up their investment by 34.6%, followed by Mexico (+34.5%), Australia (+29%) China (+25%), Singapore (+20%), Argentina (+19%), and the US (+19%).
6. **Companies now allocate the largest share of their cybersecurity investments to technology (37.9%), followed by people (33.8%), and process (28.4%).** Next year, firms will allocate more to technology (39.3%) and process (30.7%), while trimming their investment in people (30%). Companies are now using a variety of technologies to help mitigate risks, including multi-factor authentication (90%), blockchain (68%), IoT (62%), and AI (44%). Over the next two years, there will be an explosion in the use of behavioral analytics (+1735%), smart grid technologies (+831%), deception technology (+684%), and hardware security and resilience (+114%).
7. **Companies with the highest cybersecurity maturity scores are in the US (107.2), South Korea (104.7), Japan (102.6), France (101.9), Australia (101.3), Spain (101.1), and the UK (100).** Firms in these countries have made the greatest progress in developing an effective cybersecurity framework. Most of the lowest scoring companies are based in emerging markets, including Mexico (96.3), India (93.7), Argentina (93.6), and Brazil (88.6), although firms in Germany (97.3) and Switzerland (96.3) also had relatively low scores.
8. **Companies are now investing more in cyber-risk prevention than in resilience.** They are putting more into the identify (19.5%), protect (25.5%), and detect (21.3%) categories of the NIST Cybersecurity Framework than into the respond (17.7%) and recover (16.2%) categories. While

companies will invest even more in protection next year (26.5%), they will also allocate more to respond (19.2%) and recover (18.1%) and less to identify (17.9%) and detect (18.3%). While many CISOs believe that prevention is better than cure, they recognize that resilience is crucial since no security system can be 100% foolproof.

9. **As cybersecurity systems mature, the probability of costly cyberattacks decline.** Cybersecurity beginners have a 21% probability of cyberattacks generating over $1m in losses vs 16% for intermediates and leaders. The costs of cyberattacks also decrease as cybersecurity matures: the costs for beginners is 0.039% of revenue ($3.9m for a $10b company) compared with 0.012% of revenue for leaders ($1.2m for a $10b company). And beginners in our benchmarking survey may be underestimating the costs due to their ineffective detection systems.
10. **Companies are reorganizing to improve cybersecurity:** Cybersecurity leaders (37%) are more likely to assign responsibility to a CISO than beginners (20%). For beginners and companies with under $1 billion in revenue, the board of directors is more likely to have primary responsibility. However, worldwide regulatory changes are making a chief privacy or data protection officer role more common and more collaborative—and sometimes integrated—with the role of the CISO, particularly in companies with over $20 billion in revenue.
11. **As firms mature in cybersecurity, the ratio of cybersecurity to technology staff drops.** One reason is that as firms install automated cybersecurity systems with advanced technology, they require fewer cybersecurity specialists. Another is that leaders make better use of cybersecurity ecosystems where they rely more heavily on partners and suppliers and outsource more of their cybersecurity work.
12. **Calculating the ROI of cybersecurity is elusive for most firms.** One stumbling block is that it is difficult to accurately measure indirect costs, such as productivity loss, reputational damage, and opportunity costs. Another is the difficulty of gauging risk probabilities and costs avoided from tighter cybersecurity. Adding to complexity, companies focus on measuring risks, and leave out the upside from improving productivity (cited by 35% of companies), profitability (22%), corporate reputations (18%), competitive positioning (16.2%), and customer engagement (11%).

"We are in a cybersecurity arms race, and the hackers are winning. Over the years, we have tested thousands of companies. There is always a way in."

Kevin Mitnick, Chief Hacking Officer and former hacker, KnowBe4

Calls to action

ESI ThoughtLab held advisory meetings and interviews with CISOs and cybersecurity experts across industries, regions, and disciplines, who offered their insights into cybersecurity best practices. Here are 10 calls to action gleaned from our research that will help firms bring their cybersecurity programs to the next level of excellence.

1. **Conduct an audit**

   Step one is conducting an audit of your current cybersecurity practices to identify areas of weakness and needs for improved practices. Assessing your approach compared with cybersecurity frameworks such as NIST can provide a valuable guide to where to begin and keep your firm in good standing with regulators. It also can be a valuable tool for communicating with senior management and benchmarking progress.

2. **Build a cybersecurity roadmap**

   Start by tying your cybersecurity risk program to the enterprise risk management process, so that it's not just IT and security people driving the risk assessment. Next, right-size your cyber program to match the risk profile and appetite of top management. Regularly test your detection and monitoring capabilities to make sure they are effective. Finally, develop key metrics so you can ensure you're achieving your goals and create a feedback loop to refine the program as it goes along.

3. **Look at cybersecurity through multiple lenses**

   The first is governance: Make sure you've got everything buttoned down—from tone at the top through to product design. The next is transactional: Determine the cybersecurity and privacy issues relating to suppliers and customers. Lastly is crisis and disputes: Prepare a solid response policy that's going to be well practiced among the core and ancillary team, including notification duties, forensics, law enforcement, PR and preparing for class actions. Look at cybersecurity not just through a risk lens, but the upside it can bring to your business.

4. **Build a cybersecurity culture**

   Cybersecurity works best when organized as a team sport—with all staff across the enterprise sharing responsibility. Companies need to develop an information security culture that is part of everything that they do, from product development to customer engagement. The right culture is the best line of defense and building such a culture starts at the top: the board and the CEO need to set the tone and provide the governance.

5. **Get the fundamentals right**

   Cybersecurity is a very complex issue, but managing it often just takes common sense. Rather than just focusing on the latest cybersecurity technologies, first make sure you are getting the fundamentals right. For example, companies need a robust and auditable control system that continuously monitors who has access to critical systems. Simple passwords are not enough; two-factor authentication and other security enhancements are essential.

6. **Change how you communicate**

   One of the challenges for cybersecurity professionals is that the cybersecurity is sometimes too technical for management teams to fully understand. Often, CISOs talk in technical jargon or just about cost avoidance—why failing to take actions might result in a regulatory fine. Framing the discussion in business terms works best—showing the ROI in terms of reduced costs, lower risks, and improvements in market share, shareholder value, and financial performance.

7. **Adopt a proactive mindset**

   Just implementing a set of tools to detect breaches puts CISOs in a reactive mode. You need to take a proactive stance in managing your security program by adopting the mindset that you have been compromised and set out every day to disprove it. You might be using the same tools, but how you go about executing on them will be different. If you're not proactive, attackers will always get in. You should assume a breach and remediate as soon as possible.

8. **Don't manage cybersecurity in a silo**

   Creating organizational structures that encourage interplay between cybersecurity and business teams is crucial. Remember that security is a holistic discipline; you need to manage both physical and cyber risks. You could have the best physical security ever—guards, gates, guns, surveillance—but if someone can access your network from the comfort of their living room, you will not accomplish anything.

9. **Every device purchase is a security decision**

   Securing your network perimeter is not enough. The office of the future is different: people are working from everywhere—when they are at Starbucks, on vacation, in transit or at home. The peripheral boundary of your network is not strong enough to protect inflows and outflows of information. CISOs need to turn their attention to users and their devices. These devices may stay in your firm for years, and their defenses may be outdated or broken.

10. **Don't make cybersecurity an afterthought**

    When creating digital products, companies need to build security into those products from the start, rather than after they are built. Cybersecurity people should be embedded in the teams that are creating products and driving digital transformation. Right now, most firms organize cybersecurity in silos, which have only a fraction of the staff of the engineering group. So often when a new product is developed, the cybersecurity may not have enough time to properly test it and fix all the issues.

About ESI ThoughtLab

ESI ThoughtLab is an innovative thought leadership and economic research firm that helps corporate, financial, and government leaders cope with transformative change. Our research focuses on the intersection of business, government, and digital transformation.

By applying analytical tools, qualitative research, and expert opinions, our firm provides actionable insights into industry, economic, regulatory and technology trends and their impact on business and the world. We specialize in creating next-generation thought leadership that combines visionary thinking with evidence-based research and innovative content delivery.

An agile, collaborative enterprise, ESI ThoughtLab draws on its in-house team of thought leadership specialists and professional economists, together with a global network of experts, survey panels, and alliance partners to conduct analysis on industries, countries, cities, and management practices. We provide end-to-end thought leadership research—from surveys, expert panels, and executive interviews to global indexes, interactive infographics, and econometric models. Our trusted ESI brand gives us extraordinary access to senior executives, policymakers and media channels around the globe.

For further information about this study and other thought leadership programs, please contact:

Lou Celi, Project Director 917.459.4616 | Lceli@esithoughtlab.com

Barry Rutizer, Client Director 917.251.4190 | Brutizer@esithoughtlab.com

Dr. Daniel Miles, Chief Economist 215.717.2777 | Miles@econsultsolutions.com

Caroline Lindholm, Project Coordinator 215.717.2777 | Lindholm@econsultsolutions.com

For the full interactive report and the cybersecurity benchmarking database, see our website: econsultsolutions.com/esi-thoughtlab/cybersecurity-imperative-2018

ESI THOUGHTLAB

Fresh thinking to stay ahead of the curve

1435 Walnut St., 4th Floor
Philadelphia, PA 19102
esithoughtlab.com