

The Cybersecurity Imperative Pulse Report

Managing cyber risks
in a world of rapid digital change



Executive Summary

June 2019

Sponsored by:

Baker
McKenzie.

 **CyberCube**

 **hp**

 **KnowBe4**
Human error. Conquered.

 **opus**

 **protiviti**
Face the Future with Confidence

 **SIA**
SECURITY INDUSTRY ASSOCIATION

 **Willis
Towers
Watson**

The Cybersecurity Imperative program was sponsored by a coalition of leading consulting firms and other providers of cybersecurity-related services and products. Each organization is an expert in its own field and provided valuable knowledge and perspectives that enhanced the research methodology, results, and best practices included in the study.

We would like to thank our sponsors—Baker McKenzie, CyberCube, HP, KnowBe4, Opus, Protiviti, the Security Industry Association (SIA), and Willis Towers Watson—as well as our partner WSJ Pro Cybersecurity and our project management team, for helping us create and conduct our original watershed cybersecurity survey and study, as well as the follow-up Cybersecurity Imperative Pulse Survey and analysis that is included in this executive summary.

1. The state of play



As cyber adversaries accelerate their attacks on businesses—and digital innovation creates new vulnerabilities—firms across industries and regions are gearing up for their battle against cybercrime, according to our recent pulse survey of companies.

In April-May 2019, ESI ThoughtLab surveyed 467 firms to gain insights into their latest cybersecurity perspectives, plans, and practices (see research background on next page). The survey revealed that on average CISOs are increasing their cybersecurity war chests by 34% in the next fiscal year, after raising investments by 17% the previous year. Some industries, such as financial services and industrial manufacturing, plan to boost spending by as much as 40% next year, and companies with over \$10 billion in sales will bolster their budgets by a hefty 49%.

For most companies, the stakes have never been higher. Our survey found that on average firms lost \$4.7 million last year, and for more than one in 10 companies surveyed that figure was over \$10 million. Losses are skyrocketing for several reasons. One is growing activity from various threat actors, including state-sponsored hackers, cybercriminals, and malicious insiders. Another is companies' higher exposure to cybercrime due to their expanding use of IoT, cloud platforms, and other IT applications that give hackers greater latitude.

Adding to their woes, CISO's cybersecurity initiatives are subject to a "balloon effect"—squeezing down on one side of the balloon causes another side to bulge. To fight back against cybercriminals, firms are typically investing 38% of their cybersecurity budgets in technological solutions. But seasoned CISOs know that a good digital defense is not enough, so they are also building a multilayered approach that includes stronger investment in people and process. Recognizing that some hackers will inevitably find a way in, CISOs are recalibrating their cybersecurity budgets to focus more on remediation.

Many CISOs believe that their investments are already paying off. Companies report a decline in the impact from untrained staff, social engineers, and unsophisticated hackers. Our survey also shows that the impact of cyberattacks from malware, phishing, and mobile phone apps decreased over the last nine months.

However, the escalation in overall cyber losses highlights that cybersecurity is an ever-evolving struggle. To come out on top, companies need to stay vigilant everywhere, since attackers are relentless in exploiting weaknesses. With limited budgets, and cyber risks mushrooming, it is paramount that organizations understand the ROI of cybersecurity so that they invest in those efforts that will result in the optimal outcome.

Research background

We carried out our cybersecurity pulse survey in April-May 2019, garnering data from 467 respondents in 17 countries. The distribution by company size was roughly similar to that of our 2018 survey, which was conducted in June-July 2018 and comprised 1,300 respondents.

Company revenues	Percentage
\$200 million to \$999 million	20%
\$1 billion - \$2.4 billion	20%
\$2.5 billion - \$4.9 billion	17%
\$5 billion - \$9.9 billion	20%
\$10 billion - \$19.9 billion	12%
\$20 billion - \$50 billion	11%
Over \$50 billion	1%

Figure 1: Survey respondents by size

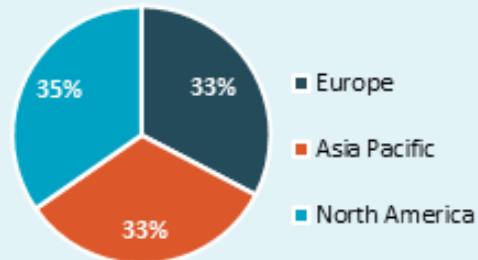


Figure 2: Survey respondents by region

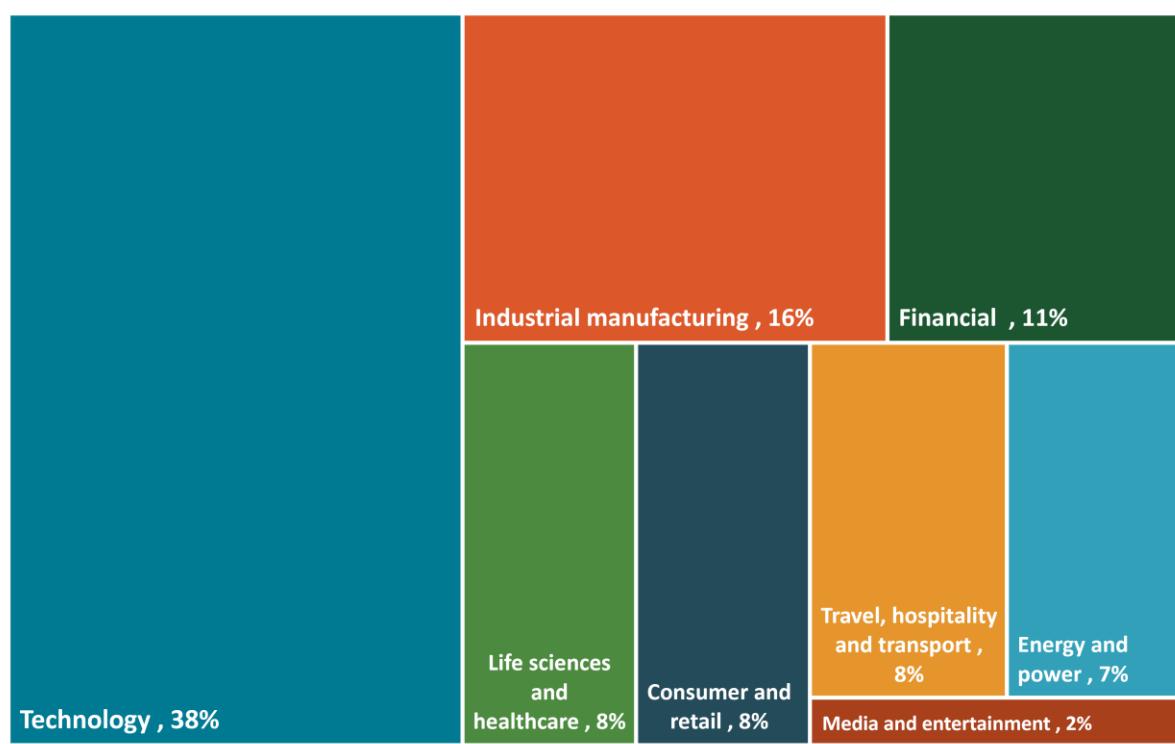


Figure 3: Survey respondents by industry

2. Threat actors on the move



As cyber threat actors become more sophisticated, organized, and prolific, companies must fight them on many fronts. Attacks continue to multiply as hackers target not just individual companies but whole industries, searching for any vulnerability.

Our pulse survey shows that companies are experiencing escalating impacts this year from key adversaries, including cybercriminals, malicious insiders, and state-sponsored hackers, often from jurisdictions beyond the reach of local law. Since last year, the percentage of companies seeing a significant impact from cybercriminal activities—such as installation of ransomware—has soared, from 57% to 71%. Attacks continue to multiply not only in number but in size and costs. Last year total malware attacks reached 857 million according to AV Test, an independent virus rating organization; in the first quarter of 2019 alone, the number rose to 901 million.

The biggest threats on the radar

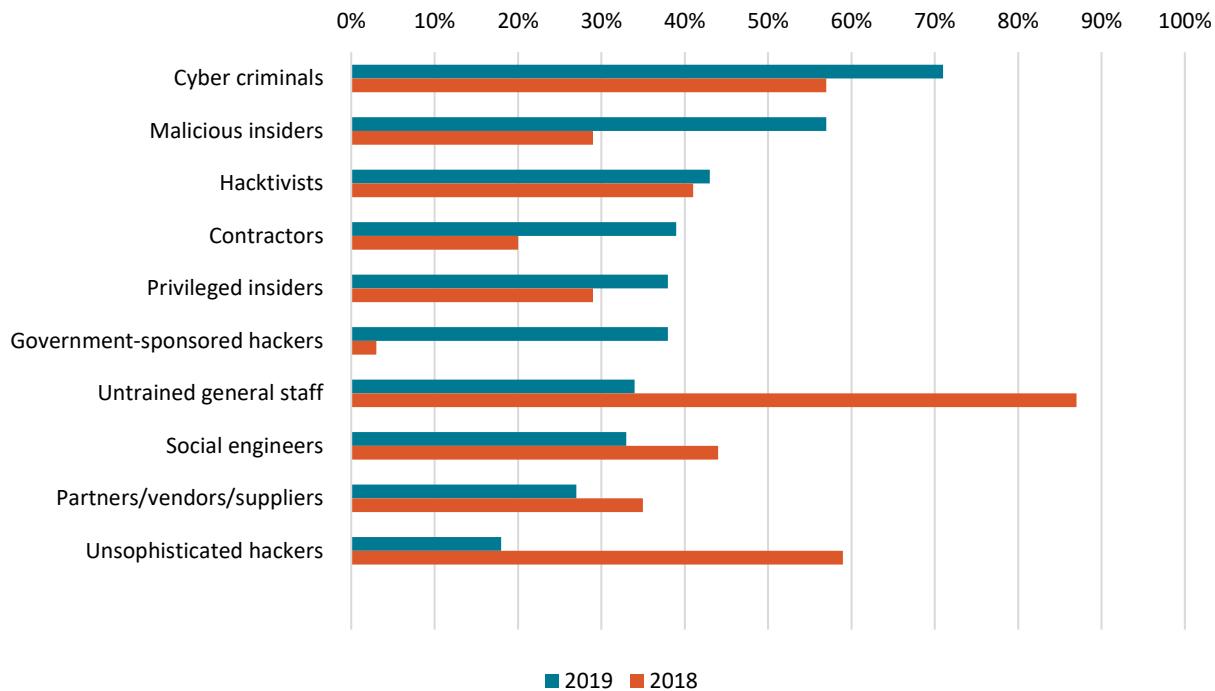


Figure 4: Which internal risks and external threats are having the largest impact on your business?

According to Brad Smith, President of Microsoft, the world is “facing a cyber-weapons arms race”, with government-backed hackers attacking users everywhere. With their sights set on intellectual property and economic gain, hackers from China, Russia, North Korea, and other countries have stepped up their strikes on companies, both large and small. In late 2018, the US Department of Homeland Security

issued a warning about nation-state hackers targeting managed service providers to penetrate their large corporate clients. Financial institutions are another favored target of state-sponsored hackers looking to profit. Our survey shows that almost half of financial firms are experiencing a large or very large impact from nation-states. “Political shifts between and within nation-states and changes to domestic and foreign policy have led to sanctions, conflicts, civil outbreaks, and warfare,” says Jason Harrell, Head of Business and Government Cybersecurity Partnerships with the Depository Trust and Clearing Corporation (DTCC). These are creating new incentives for retaliation by threat actors.

Firms in some countries, particularly France, Germany, and India, see a greater risk from state-sponsored hackers. In France, Russian attempts to manipulate the last presidential election raised awareness across the public and private sectors. In August 2018, North Koreans hacked the systems of India’s Cosmos Bank and siphoned off nearly \$13.5 million through simultaneous withdrawals across 28 countries.

“Cyberattacks against the financial system provide yet another vehicle for nation-states and other well-funded threat actors to respond to political shifts and policy changes.”

Jason Harrell, Head of Business and Government Cybersecurity, DTCC.

Over the last year, surveyed companies report that the impact from malicious insider threats has doubled, with 57% now citing a large or very large impact (versus 29% in our 2018 survey). In the past, organizations underestimated the impact of insider threats, but they are also worsening as technology—particularly the cloud—makes data more accessible and its movement easier. Attacks by state-sponsored hackers are also often made possible by collaboration with insiders. Although the number of insider attacks is rising, the ability of companies to mitigate them is improving. With more sophisticated systems in place, firms are better equipped to detect, analyze, and respond to insider attacks.

At the same time, companies are making progress in addressing previous areas of high cyber risk. For example, firms report a notable reduction in the risk from untrained staff, last year’s greatest threat, with the share of firms reporting a large or very large impact from untrained staff down from 87% in 2018 to 34% currently (see Figure 4). Over the last year, widespread awareness of the cyber risks from careless staff led many companies to invest more in defenses against human error and to install enterprise training programs. This has reduced the number of untrained staff and costly errors by employees.

“As we go deeper into the digital age, cybercriminals are becoming much more sophisticated and well-funded. Companies and industries that have never had to deal with such risk before are now having to prepare.”

Brian Hengesbaugh, Partner and Global Chair of Data Privacy and Security, Baker McKenzie.

While some of these survey results may reflect wishful thinking on the part of business executives, it has been shown that effective training can clearly make a difference. For example, Verizon’s 2019 data breach report reveals that the percentage of employees clicking on simulated phishing emails during security awareness tests dropped to about 3% in 2018 from about 8% in 2016 and from 25% in 2012. Nonetheless, security controls in all areas of the environment—whether employees, third-party suppliers, or other external actors—must be strengthened.

3. Shifting modes of attack



This year, firms are seeing a lower impact from the threats they worried about most in 2018, such as malware and phishing. But others, such as attacks through ecosystems, are rising—an example of the “balloon effect,” as squeezing down on some threats means increases in others.

Since our last survey, organizations have done much to counter the types of attacks that gave them the most trouble last year. These include malware, phishing, mobile apps, web apps, and embedded systems. CISOs' efforts have paid off: the impact they report from these types of attacks has declined materially over the last year (see Figure 5).

But these same firms are seeing a greater impact from attacks in other areas, including denial of service, abuse of legitimate or privileged access, and lost/stolen devices. Companies are also experiencing rising threats both to and from the ecosystems that they rely on to digitally transform.

There are considerable variations in cyber incidents by industry. The energy and financial sectors are sustaining major impacts from a wide range of attacks, while the media and travel industries have suffered much less. For example, half of energy companies saw a large impact from attacks through ecosystems, compared with 26% of media and entertainment firms. Likewise, 43% of financial firms report a large impact from abuse of legitimate access, versus just 20% of travel, hospitality, and transport firms.

Survey respondents in India report they are among the hardest hit from all types of intrusions, particularly through supply chain, mobile apps, and malware/ransomware. In fact, the country is among the least cyber-secure in the world, with a high level of successful attacks. Last year, the breach of the Aadhaar database, India's biometric ID system, was considered the world's largest, compromising the records of more than one billion registered citizens.

“The issue for energy companies is that they are slower moving. They don't have the mature, third-party security programs that other industries have been forced to develop, such as the banking and finance industry.”

Dov Goodman, Director of Risk and Compliance, Panorays; previously with Opus.



Attacks from many directions

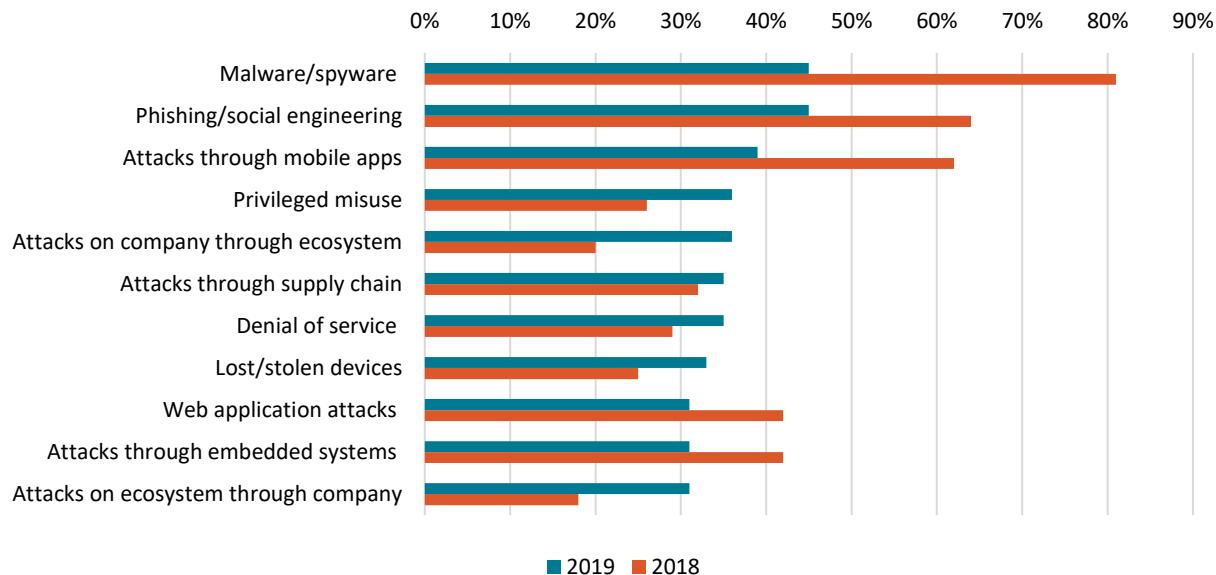


Figure 5: Which of the following cybersecurity attacks are having the largest impact on your business now?

Most pulse survey respondents are confident about the future, expecting a lower impact next year from most types of attack (see Figure 6). This is a turn from last year's survey, when respondents were expecting big shocks from many types of attacks. CISOs believe that their increased investments in cybersecurity programs will help them mitigate the escalating dangers ahead. It remains to be seen whether their expectations are justified.

Next year looks brighter

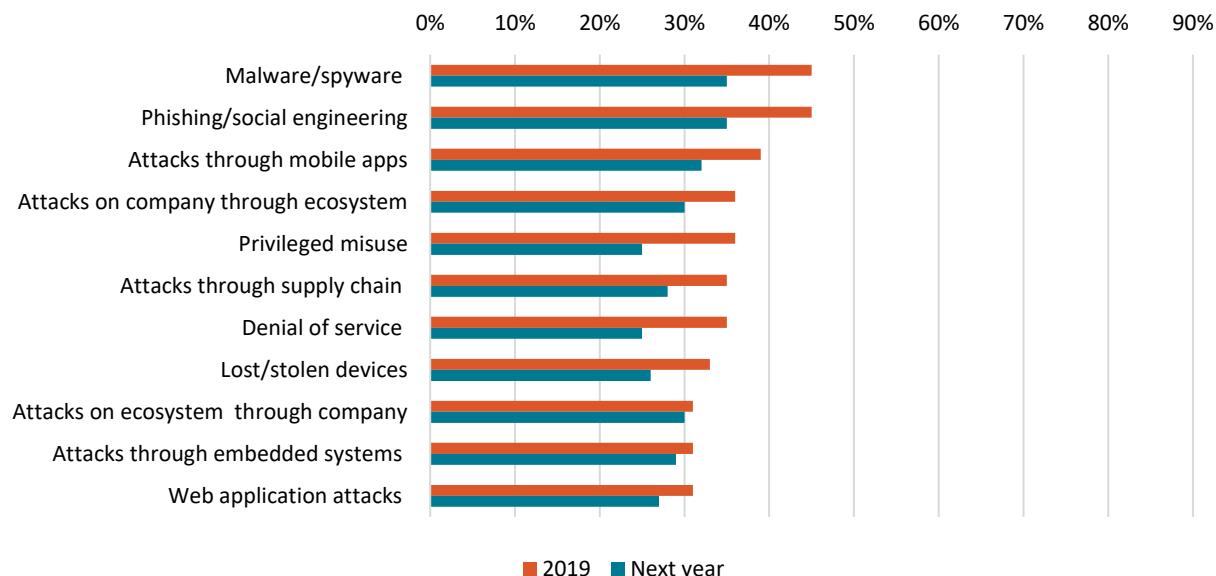


Figure 6: Which of the following cybersecurity attacks do you expect will have the largest impact over the next year?

4. Growing vulnerabilities



Since our last survey, companies report greater vulnerabilities to cyberattacks, through entry points including email servers, enterprise mobile connections, web-facing apps and legacy IT systems. Over that period, the only vulnerabilities to lessen were shadow IT and emerging technologies.

Currently, companies see the Internet of Things and shadow IT (unapproved IT) as their biggest vulnerabilities, followed by email servers, employee-owned devices with network access, and enterprise mobile connectivity. Third-party systems with network access are also worrisome for companies, as is cloud infrastructure (see Figure 7).

The rapid pace of innovation increases corporate cyber risk if safeguards are not built in upfront. This is especially true for IoT, cloud, and other emerging technologies. Even much older technologies such as email servers, desktops and laptops, and out-of-date software, along with weak authentication methods and user error, can expose companies to greater risks.

“Today you rarely find any device that in some way cannot communicate with a server, and most embedded infrastructure has some type of internet connection as interconnected systems become more prevalent.”

Joe Gittens, Director of Standards, Security Industry Association (SIA).

Digital transformation creates vulnerabilities

Vulnerabilities	2019	2018
"Internet of Things" (IoT)	33%	n.a.
Shadow IT	30%	33%
Email servers	28%	10%
Employee-owned devices with network access	28%	7%
Enterprise mobile connectivity	28%	23%
Systems owned by third-party suppliers and partners with network access	27%	n.a.
Cloud infrastructure and applications	27%	8%
Emerging technologies (AI, blockchain, telematics—for 2018, included IoT)	23%	48%
Network-connected building systems	22%	n.a.
Web-facing applications and infrastructure	22%	15%
Company-owned desktops and laptops	21%	8%
Legacy infrastructure and applications	19%	8%
Printers and other embedded infrastructure	17%	4%

Figure 7: Which areas of your organization's IT infrastructure do you believe are most vulnerable to cyber risk?

Largest vulnerabilities by industry

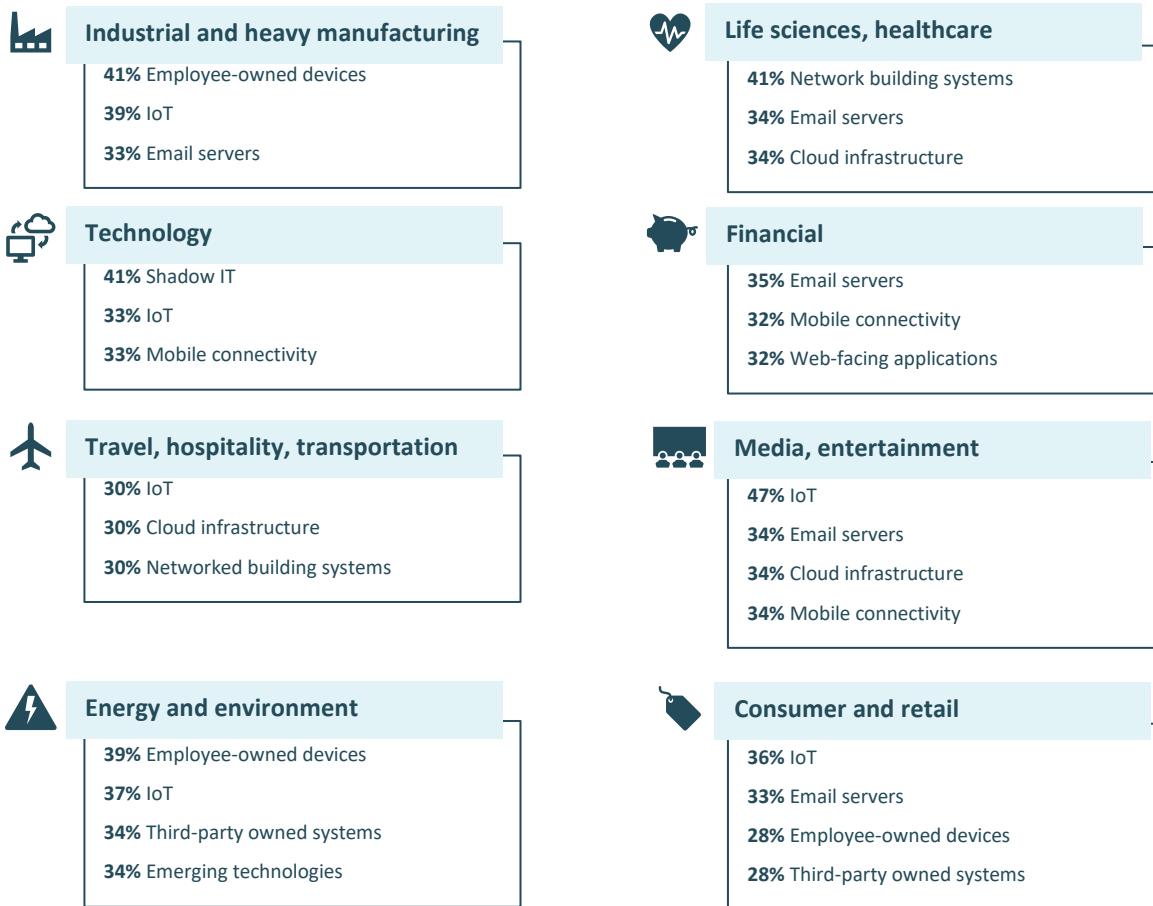


Figure 8: Which areas of your organization's IT infrastructure do you believe are most vulnerable to cyber risk?

Yet companies are getting smarter at identifying vulnerabilities. Over the last year, firms allocated almost a quarter of their cybersecurity budgets to risk identification, including better techniques for assessing asset vulnerabilities and supply chain weaknesses. CISOs plan to continue to invest at similar levels next year, particularly as the use of digital technology and ecosystems of partners and suppliers expose companies to new dangers.

Of course, vulnerabilities vary depending on the industry (see Figure 8). Industrial manufacturing and energy firms find IoT, for which usage is exploding, and employee-owned devices with network access as the biggest risks. For these companies, sensor-based systems are often sourced on price, rather than security—a problem that companies are now recognizing due to several high-profile attacks through these devices.

For the tech industry—where many employees have the skills to build their own systems and software—shadow IT is the largest worry. Compare that with media/entertainment companies, which are most concerned about IoT vulnerabilities given their growing use of IoT to gather and use data. (Disney has already invested over \$1 billion in IoT to provide customers with a connected experience at its amusement parks.) Life sciences and healthcare companies, which include highly networked facilities such as hospitals, see internet-connected building systems as their biggest vulnerability.

“Applying insights from unique sources of data behind the firewall can help inform a company on its cyber exposure and defense stance, compared with its peers. These insights are helping companies to make better decisions on which risks to control, mitigate, or transfer to other parties—including insurance.”

Rebecca Bole, Head of Industry Engagement, CyberCube Analytics.

5. Rising costs of cyberattacks



Since last year, companies report higher losses from cyberattacks. These revised costs are in line with increases in the number and size of cyberattacks across industries. But they also reflect improved corporate systems for detecting breaches and measuring costs.

According to our latest survey of companies, on average annual losses from cyberattacks grew to \$4.7 million last fiscal year—with more than one in 10 companies losing more than \$10 million. That amount equates to an average of 0.114% of revenue across all firms surveyed. Our analysis shows that cybersecurity losses are more severe for mid-sized companies (0.259% of revenue) than for large companies (0.076%) and very large companies (0.042%). (See Figure 9.)

Cyber losses by company size

	Average revenue	Average loss	Loss as % of revenue
Mid-size	\$600 million	\$1,556,250	0.259%
Large	\$4.4 billion	\$3,309,375	0.076%
Very Large	\$26 billion	\$10,773,423	0.042%
Average	\$8.75 billion	\$4,738,115	0.114%

Figure 9: Over the last fiscal year, what was your total cost for cyber loss events as measured by your company?

The size of cybersecurity losses also varies considerably by industry. Companies in the energy sector were the hardest hit in the last fiscal year, with losses averaging 0.176% of revenue. Cyberattacks on the energy industry have been steadily increasing over the past several years. The oil and gas sector, particularly, has lost billions of dollars, and this year, for the first time, an assault on the grid interrupted power flow at a facility in the US. Losses are lowest in life sciences/healthcare, at 0.083% of revenue, despite the ransomware attacks that some hospitals have suffered in the past few years (see Figure 10).

Cyber losses by industry

Industry	Average revenue	Average loss	Loss as % of revenue
Energy	\$8.9 billion	\$5,088,157	0.176%
Consumer	\$6.6 billion	\$3,323,611	0.161%
Technology	\$8.4 billion	\$5,222,154	0.123%
Media	\$5.1 billion	\$3,632,894	0.110%
Industrial manufacturing	\$9.4 billion	\$3,526,315	0.106%
Travel, hospitality, transport	\$8.4 billion	\$2,926,875	0.097%
Financial	\$12.8 billion	\$7,173,264	0.084%
Life sciences	\$6.9 billion	\$4,949,431	0.083%
Average	\$8.75 billion	\$4,738,115	0.114%

Figure 10: Over the last fiscal year, what was your total cost for cyber loss events as measured by your company?

In the last fiscal year, companies in the US bore the largest losses, at 0.164% of revenue on average, followed by firms in Germany (0.123%) and the UK (0.123%). (See Figure 11 for the full costs by country.) According to a recently released report from the White House's Council of Economic Advisors, the US economy may have lost as much as \$109 billion in 2016 due to cyberattacks, and pundits believe that growing geopolitical tensions with the US are leading several nation-states to accelerate cyberattacks. Cyber risks are also rising in the UK; the National Crime Agency recently reported that cybercrime now accounts for more than half of all crime in the UK.

However, it is important to note that the average size of the surveyed companies in the US and UK is smaller than the average for the overall survey sample, which may magnify cost estimates as a percentage of revenue. Conversely, the size of surveyed firms in India—a country known for its inadequate cybersecurity—is greater than the average for our overall sample, which may lead to an understatement of the cost of cyber losses.

The higher cost percentage for Germany, where the average sample company size is close to that for the overall sample, highlights that nation's systemic problem with cybersecurity. Well-publicized cyberattacks that released the personal data of thousands of German public figures convulsed the country earlier this year. It spurred soul-searching about the country's lag in cyber-awareness, which some have attributed to traditionalism and skepticism about digital innovation among corporate executives.

Cyber losses by country

Headquarters country	Average revenue	Average loss	Loss as % of revenue
US	\$6.2 billion	\$4,101,814	0.164%
Germany	\$8.6 billion	\$6,766,847	0.128%
UK	\$4.4 billion	\$3,935,964	0.123%
France	\$7.7 billion	\$3,065,306	0.099%
China	\$9.8 billion	\$4,286,111	0.090%
Japan	\$12.5 billion	\$5,350,000	0.085%
India	\$14.7 billion	\$6,505,376	0.080%
Average	\$8.75 billion	\$4,738,115	0.114%

Figure 11: Over the last fiscal year, what was your total cost for cyber loss events as measured by your company?

Our pulse survey shows that most companies across industries and regions are upping their estimates of losses for several reasons. First, they are witnessing a greater volume of cyberattacks and higher losses per incident. Second, they are doing a better job of measuring their losses—not just direct costs, such as financial expenses and fines, but also indirect ones such as opportunity costs, reputational costs, and loss of customers and future sales.

Nonetheless, measuring incident losses and the potential risk of losses is a tricky business. According to Vince Dasta, Associate Director at Protiviti, direct or primary losses are generally understood and contained, whereas secondary losses related to outside stakeholders can be highly variable and expensive.

The timing of impacts from cyber breaches makes measurement even more complex still. Take for example the damage to a company's reputation after it suffers a cyberattack. How long will the damage last? Will consumers quickly forget about the incident, or will the company lose customers permanently? Another example is intellectual property theft. Sometimes it may take more than five years for a company to feel the full consequences on its business, but the costs might be very large, particularly if a company has lost market leadership as a result.

“Secondary costs such as those from consumers, outside forensics experts, legal counsel, regulators, and even PR firms can add up very quickly.”

Vince Dasta, Associate Director, Protiviti.



Where the losses are generated

The pulse survey shows that the costs of cyberattacks are fairly evenly spread among different categories. These include direct losses from theft, fines, and compensation; indirect losses relating to reputation and opportunity costs; and spending for response and recovery.

Pulse survey respondents report that the largest costs came from response/recovery and from productivity losses, and the lowest are related to indirect financial costs, and fines and legal costs (see Figure 12). The survey shows a growing recognition of indirect costs that are harder to quantify. For example, in 2018, 20% said they did not measure opportunity costs, 11% did not measure productivity losses, and 20% did not measure reputational costs.

Losses by category

Technical response costs (investigation, remediation, recovery)	12%
Productivity loss—staff downtime due to operation interruption, lost wages	11%
Direct financial costs—financial theft, monetary compensation to victims, etc.	10%
Replacement costs—repair/replace capital assets, recover data, etc.	10%
Customer response costs (cost of notifying customers and stakeholders)	10%
Reputational costs—reduced market share, increased cost of capital, loss of sales, etc.	10%
Opportunity costs—loss of business gains from diverting management attention	10%
Intellectual property costs—business impact from loss of IP and confidential data	9%
Indirect financial costs—loss of customers, loss of future sales	9%
Fines and legal costs—rounds of litigation, liability risks, regulatory fines, etc.	8%

Figure 12: Roughly what percentage of these costs came from the following types of cyber incident losses over the last 12 months?



6. Bigger cybersecurity budgets



Companies boosted their cybersecurity budgets by 17% last fiscal year, and they plan to double that increase to 34% next year to protect against rising threats and vulnerabilities. About 12% of firms surveyed plan to amplify their budgets by more than 50% next year.

With business conditions still strong, companies are allocating more resources to a better cybersecurity defense as awareness of the magnitude of the problem grows.

Regulatory pressures are also having an effect. The European Union's General Data Protection Regulation (GDPR), for example, came into effect in May 2018. It requires organizations to disclose data breaches within 72 hours of discovery, which means they will become public knowledge and require more investment in compliance and remediation.

California's data privacy law will come into effect in January 2020, and New York State continues to phase in strict cybersecurity regulations for the financial sector implemented in 2017.

“Cyber risk challenges organizations across all verticals and geographies; significant increases in budgets highlight the determination of companies to do something about it.”

Rob Sloan, Cybersecurity Research Director, WSJ Pro.

All industries are upping their game

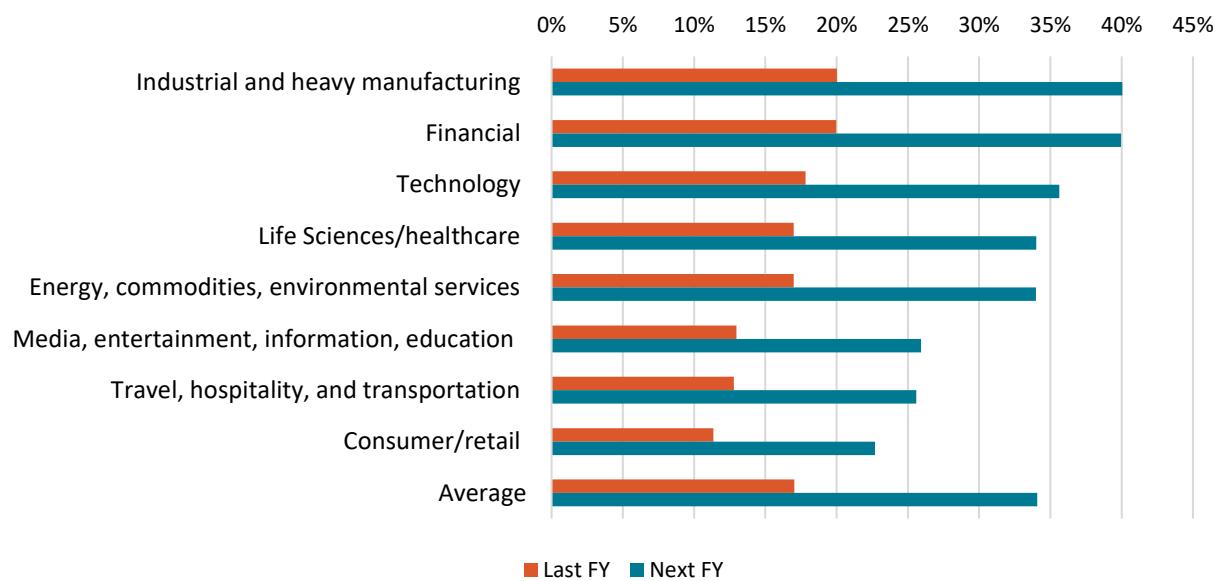


Figure 13: How much did your cybersecurity budget rise over the last fiscal year, if at all? How much do you expect it to rise over the next fiscal year, if at all?

The financial sector is increasing its spending on cybersecurity particularly fast, expecting a jump of 40% next year, according to our pulse survey (see Figure 13). The same is true for the industrial and heavy

manufacturing sector, which has been lagging in cybersecurity but now finds itself a target for ransomware and state-sponsored attacks. Its vulnerabilities are also increasing through its ever-expanding supply chains and ecosystems as well as escalating use of Internet-connected sensors that often lack security features.

Even with these richer budgets, companies may not be spending enough to win the arms race with hackers, particularly in some industries. Given their relatively high vulnerability and costs from cyberattacks, many media companies appear to be underspending relative to other firms. Consumer/retail companies are in a similar situation (see Figure 14).

Comparing costs and spend

Industry	Cost as % of revenue	Increase in spend next year
Life sciences	.071%	34%
Media	.071%	26%
Technology	.062%	36%
Energy	.057%	34%
Financial	.056%	40%
Consumer/retail	.051%	23%
Industrial manufacturing	.037%	40%
Travel, hospitality, transport	.035%	26%
Average	.055%	34%

Figure 14: How sector plans for cybersecurity spending stack up against their costs.

7. Recalibrating cybersecurity investments



To win against hackers, companies need a multi-layered defense. CISOs are allocating the biggest part of their budgets to technology and are seeking the right balance between investments in people and process. They are also recalibrating their investments to focus more on identification and resilience.

Compared with 2018, the pulse survey shows a slight trend away from investment in people and toward process, which was previously underfunded (see Figure 15). With cyberattacks an ever-present danger, CISOs are making sure that their companies have effective processes and plans in place to detect, prevent, and respond to cybersecurity incidents. These processes include improved cybersecurity data and analysis, and better procedures for prioritizing assets and measuring impacts.

For next year, firms indicate an uptick in emphasis on people, particularly in consumer markets, and media and entertainment. This includes recruitment of cybersecurity specialists, which remains a challenge across industries.

Finding the right investment balance

Category	FY 2017-18	FY 2018-19	FY 2019-20
Technology	38%	38%	38%
People	34%	31%	32%
Process	28%	31%	30%

Figure 15: What percentage of your cybersecurity budget over the last year has been devoted to people, process, and technology? What about for the next fiscal year?

Companies are also adjusting their investments across the NIST framework of identify, detect, protect, respond, and recover. Recognizing that no cybersecurity system is foolproof, CISOs have increased their investment in response over the last fiscal year and plan to continue to budget more over the next year. Nonetheless, response and recovery will remain less funded than other NIST categories. This may create future problems for organizations, since inadequate response and remediation not only lead to high direct costs, but also can have serious implications for customer retention and reputation.

The most striking change, however, is in risk identification, an area where most companies expected to cut back investment but are instead increasing it. The reason: CISOs increasingly understand that the speed and complexity of digital innovation and strategic transformation will continuously expose them to new risks and vulnerabilities. For savvy CISOs, risk identification is not a one-and-done initiative but an ongoing process.

Adjusting budgets across NIST categories

NIST Category	FY 2017-18	FY 2018-19	FY 2019-20
Identify	23%	23%	22%
Detect	22%	20%	19%
Protect	22%	22%	22%
Respond	17%	18%	18%
Recover	15%	17%	18%

Figure 16: What percentage of your cybersecurity budget over the last year has been allocated to the five main areas of cybersecurity (as identified by the NIST framework)? What about for the next fiscal year?



8. Calls to action



As losses from cyberattacks rise across industries and regions, management teams are approving larger budgets for cybersecurity. But CISOs need to ensure they are making the right investments in technology, people, and processes that will provide their firms with the best performance outcomes.

- **Make sure you are investing enough in cybersecurity.** Some industries, such as media and consumer markets, lag in cybersecurity and may be caught unprepared when hackers turn their attention to them. Smaller firms are particularly exposed. “Investment in proactive deterrence is key,” says Gittens of the Security Industry Association. “The cost of recovery is very high, so it is critical that companies invest more to build resiliency, harden their products and systems to make security breaches more difficult, and thereby protect themselves from the time and expense of recovery. They must invest to make their ‘crown jewels’ tougher to get to.”
- **Know that cybersecurity technology is not enough.** In today’s arms race, investing in the latest technology is vital but it is not sufficient. You need to take a multilayered approach, carefully calibrated to include adequate attention to both people and process. “Technology alone is not enough to manage cyber risk—it never was and never will be,” says Sloan of WSJ Pro. “Organizations need an approach that balances people, process, and technology in a way to maximize operational effectiveness at quickly identifying, investigating, and countering attacks.”
- **Understand that the cybersecurity war must be fought on all fronts.** Don’t forget the balloon effect: when you push down on one type of threat, others will take their place, whether internal or external, malicious or not. You need to be as relentless as your attackers. “Cybersecurity is like a game of whack-a-mole,” says Dasta of Protiviti. “A company cannot fully anticipate where the next threat or highly motivated cybercriminal will come from. Therefore, it needs a solid base of cyber hygiene along with a good response plan to deal with unanticipated events.”
- **Think of cybersecurity like any other existential threat to your business.** The risks are not just about privacy, liability, and stealing data. “Companies need to look at cyber threats in business terms: these are operational risks that can cause interruptions and impact a firm’s ability to deliver its core products and services,” says Dasta. Understanding the operational risks may require different types of analysis to assess the full business impacts.
- **Pay particular attention to risks from third parties and your supply chain.** Firms are focusing more on their core functions and increasingly outsourcing others to third-party service providers. “This expansion of the supply chain increases the surface area for potential threat actors to gain access to a firm and create harm,” says Harrell of DTCC. Addressing third-party—and even fourth-party—risk should be part of any defensive plan. Sloan agrees, noting that, despite progress being made to train staff and secure networks and data, security professionals must also look beyond their own organizations to ensure third parties are equally diligent in

their cybersecurity practices. What should CISOs do? Adopt approaches that will scale to the full supply chain, not focus just on the critical relationships at the top of the “supply chain risk pyramid”, which are generally large suppliers that are “buttoned up and effective at cybersecurity”, says Goldman of Panorays. “To reach the middle and lower levels of the pyramid will require automation, as human beings will not be able to adequately monitor and assess what may be thousands of less-critical supplier and vendor relationships,” he adds.

- **Be aware that legal and regulatory risks are also rising substantially.** As governments implement regulations designed to protect against data breaches, companies that do not comply with the new standards face hefty penalties and legal consequences, according to Hengesbaugh of Baker McKenzie. He cites the EU’s GDPR, a new privacy law in Brazil, and California’s new Consumer Privacy Act. “The risk associated with not having appropriate security is increasing dramatically,” he says.
- **Conduct a robust data mapping exercise.** To mitigate the impact of cyber incidents, you must identify where you have sensitive and personal data, not only in your own enterprise but also where it is going to third-party vendors. Vulnerabilities should be identified across the whole supply chain. Hengesbaugh suggests asking these tough questions: Do we have to keep all the sensitive data we have? Do we have to keep it as long as we do? How can we quickly lock it down? How strong is our oversight over our vendors to ensure they are protecting the data?
- **Implement rigorous incident training.** To do so, put key stakeholders through a strong scenario exercise to prepare them for events when they occur, and to plan on how to respond quickly. According to Hengesbaugh, a speedier response also will likely limit any potential legal damages or penalties levied by regulators.
- **Assess and quantify your cyber risk.** Leading companies utilize innovative security tools to improve the assessment of their overall cyber loss potential, as well as decision support to optimize any cyber risk transfer strategy, according to Peter Foster, Executive Vice President with Willis Towers Watson. “Such analysis helps facilitate the prioritization of cybersecurity investments to ensure that they have the greatest impact on risk mitigation,” he says.
- **Measure your full losses, costs, and returns.** When you are hit by a successful cyberattack, in order to take the best approach to remediation, you need to understand all your costs—both direct and indirect, tangible, and intangible. By having a strong grip on the ROI on your investments, you can ensure that you are getting the most out of your cybersecurity budgets.

Despite considerable progress over the last year, cybersecurity is still more of an art than a science. To fully optimize their investments, CISOs need better benchmarking data on budgets, practices, plans, and performance outcomes for their industry. Filling this major cybersecurity data gap will be the subject of our upcoming 2019 cybersecurity research initiative: *Driving Cybersecurity Performance*. Stay tuned!



Lou Celi | **Phone:** 917.459.4614 | **Email:** Lceli@esithoughtlab.com

Barry Rutizer | **Phone:** 917.251.4190 | **Email:** Brutizer@esithoughtlab.com