



ESI THOUGHTLAB

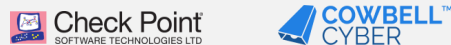
Driving Cybersecurity Performance

*Improving results through
evidence-based analysis*

Lead sponsors



Supporting sponsors



Media partners



Project advisors



START ►

Introduction

Digital innovation is a double-edged sword: while essential for driving performance in today's interconnected world, it exposes firms to greater cybersecurity risks. The greater reliance on technology during the COVID-19 pandemic, combined with a rise in opportunistic cyberattacks, has served as a stress test for cybersecurity systems.

COVID-19 has fast-tracked digitalization as businesses turn to remote working, e-commerce, cloud platforms, and other technology-enabled solutions to cope with the rigors of social distancing. For many firms, the crisis has exposed the weaknesses in their ability to detect, protect, and respond to cybersecurity threats, particularly in times of business disruption, when IT resources are diverted, and work shifts to outside an organization and a quickly blurring perimeter.

But the pandemic is more than a test: it is the accelerant for the next phase of the digital revolution. Many of the digital solutions embraced during the crisis will gather momentum in the post-COVID-19 environment. As a result, cyber risks will become more pervasive and complex, while cybersecurity effectiveness and resilience will become levers of competitive advantage. Although firms have made major improvements in cybersecurity, there is more to be done. CISOs need to revise their cybersecurity strategies to encompass proactive prevention along with a deep understanding of the risks their companies face and the heightened nature of today's sophisticated cyberattacks.

To help CISOs do that, ESI ThoughtLab worked with a coalition of cybersecurity, cyber insurance, and technology experts from leading companies and associations to answer a central question: How can firms drive the best cybersecurity performance in today's complex digital world? To answer that question, we conducted a comprehensive benchmarking study covering the cybersecurity investments, practices, plans, and performance results of 1,009 companies across 13 industries and 19 countries.

This eBook provides insights into how cybersecurity leaders organize for success, where they invest, and which technologies, processes, and analytical tools they use. With budgets coming under greater pressure in the pandemic era, this research should help your firm optimize the use of its cybersecurity resources for the challenging times ahead.



**Lou Celi, Chief
Executive Officer
ESI ThoughtLab**



**Daniel Miles, PhD
Chief Economist
ESI ThoughtLab**



Research background and methodology

Our analytical approach

To conduct our cybersecurity analysis, ESI ThoughtLab's team of economists and digital specialists used a rigorous, mixed-methods research approach that included the following elements:

- **A cross-industry survey of 1,009 companies** to collect internal cybersecurity benchmarking data and insights into their cybersecurity approaches and results.
- **Cost-benefit analysis** to quantify the full direct and indirect impacts of cybersecurity investments and strategies on costs and revenue.
- **ROI modeling** to measure the impact of cybersecurity investments on risk probabilities and reduction in the number and size of losses.
- **Quantitative correlations** of cybersecurity data provided by Verizon Business, split by company, with our survey output to provide another lens for analyzing effectiveness and maturity.
- **Input from a high-level advisory board** of industry executives and cybersecurity experts to shape the research agenda, analyze the survey results, and validate the research findings.
- **In-depth interviews with 20 cybersecurity thought leaders**, including CISOs and other senior executives across industries as well as cybersecurity experts from around the world.



Survey methodology and profile

ESI ThoughtLab conducted a comprehensive benchmarking survey of executives at 1,009 companies across 13 industries and 19 countries. It was carried out over the phone from November 2019 to January 2020.

Respondents had responsibility for cybersecurity or detailed knowledge of its use. More than 9 in 10 were C-level executives.

The survey examined cybersecurity investments, plans, practices, and performance results at their firms. It included quantitative questions to allow ESI ThoughtLab economists to develop a rigorous cybersecurity maturity framework, analyze performance metrics, benchmark practices, and measure the ROI on cybersecurity investments.

Companies in survey sample

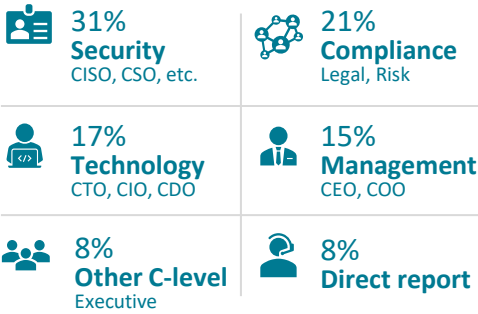
\$15tn
combined revenue

\$6.2tn
contribution to
global GDP

7%
contribution as a share of
global GDP

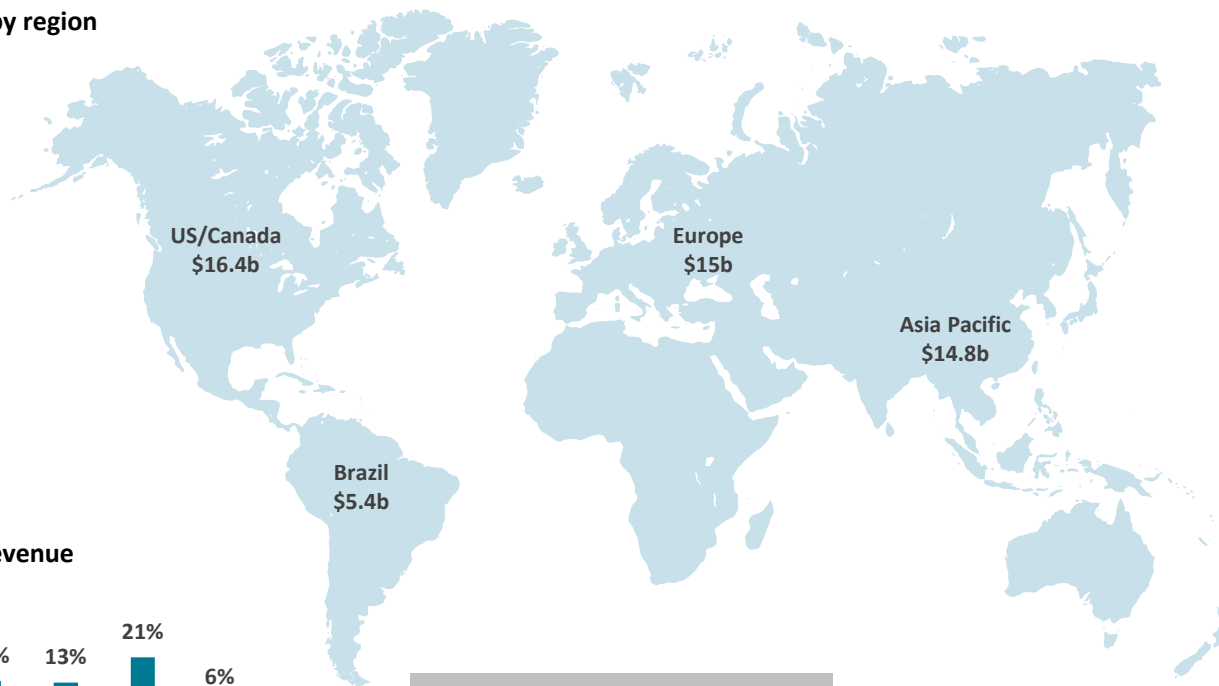


Respondents by function

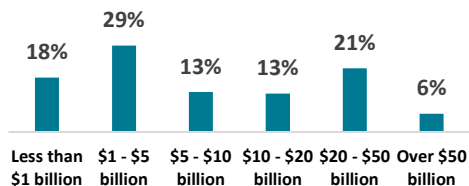


Respondent profile

Average revenue by region



Respondents by revenue



Total cybersecurity spending of all companies in sample
\$9.7b

Countries

Americas 37%

Brazil
Canada
US

Asia Pacific 26%

Australia
China
Hong Kong
India
Japan
South Korea

Europe 37%

France
Germany
Italy
Netherlands
Nordics*
Switzerland
UK

*Denmark, Finland, Norway, and Sweden



Executive summary

Executive summary

The ROI on cybersecurity

ESI ThoughtLab's study of 1,009 worldwide firms in 13 industries found that CISOs, on average, gain a massive ROI of 179% on their digital investments. To achieve these returns, CISOs need to construct resilient cybersecurity programs built around evidence-based analysis and a deep understanding of the evolving risks they face.

The rise in cybersecurity investment

Digital transformation continues to expose companies to new risks and vulnerabilities as they adopt emerging technologies, digital processes, and new business models. The COVID-19 pandemic is accelerating these trends as companies embrace remote working and rethink supply chains, and as consumers ramp up their use of digital shopping and banking, as well as remote medicine, communication, and entertainment.

To cope, companies are investing more in cybersecurity, with an average increase of 12% in 2019 and 14% targeted for 2020, although these budgets may change as the pandemic plays out. In 2019, the companies in our sample spent about \$9.6 million each on cybersecurity, about \$515 per employee. Cybersecurity leaders, those firms most advanced in cybersecurity effectiveness and compliance, spent far more: \$15 million, or about \$618 per employee. The largest share of investment budgets went to technology (39%), followed by people (32%) and process (28%). This spending pattern held relatively constant across companies of different sizes, industries, and cybersecurity maturity.

The payback on cybersecurity

On average, firms see an overall ROI of 179% from their cybersecurity investments. That means that every dollar of investment generates almost \$2 in benefits. ROI on investments ranges from 271% for investments in people, to 156% for process, and 129% for technology. The least cyber-mature firms recognize the highest ROI, since they take basic steps that can have outsized benefits. Companies experience diminishing returns as they become more cyber mature. In all, the additional cybersecurity spending last year by the 1,009 firms we surveyed—which amounted to \$1.4 billion—has enabled them to reduce their combined potential losses by an estimated \$3.9 billion.

Our study of 1,009 firms found that greater investment in cybersecurity generates an ROI of 179%, close to \$2 in benefits for every \$1 spent.

Executive summary

The cybersecurity imperative

Companies need to do more

Despite their investments, our 1,009 respondents lost \$4.1 billion from cyberattacks in the most recent year, an average of \$4.1 million per firm. The losses stemmed from 28,100 successful breaches, averaging about \$330,000 per breach. While the lion's share of these breaches were minor (meaning they affected only a small number of people and machines), about 20% of breaches were moderate and about 1% were material (defined as generating a substantial loss and requiring disclosure to a third party). Insurance and financial firms suffered the most attacks, and financial, retail, hospitality, and automotive firms sustained a disproportionate number of material breaches.

Even before the pandemic, the greatest losses came from malware (66%), phishing/social engineering (60%), and password/credential reuse (49%). Cyber criminals were seen to be the biggest threat actors. As business goes more digital over the next two years, executives also expect an increase in attacks through artificial intelligence (38%), denial of service (34%), and web applications (29%). With geopolitical and social unrest growing, and greater economic volatility ahead, firms are bracing for a rise in cyber terrorism and attacks from nation-states. For many CISOs, the challenge will be how to do more, with potentially less, if budgets are streamlined for the post-pandemic aftermath.

Taking cybersecurity to the next level

Adding to the complexity, companies have tended to underestimate their exposure to breaches. While the average firm in our study assigns a 45% probability to experiencing a moderate or material breach in 2020, our analysis shows a much higher probability, ranging from 62% to 86%.

To reduce risk probabilities, CISOs must go well beyond compliance with cybersecurity frameworks, such as NIST, ISO, and others. For example, only 64 of 151 companies (42%) that evaluated themselves as NIST compliant are rated as being leaders in their cybersecurity practices in the study. Rather than applying NIST as a box-ticking exercise, cybersecurity leaders need to better align such frameworks with their business goals, strategies, and individual risk profiles. Cybersecurity leaders, more than others, tend to combine analysis from advanced quantitative tools and input from internal business partners and third-party experts to make the best decisions.

CISOs in our study assign a 45% probability of a moderate or material breach. Our analysis shows that the probability is considerably higher: 62% to 86%.

Executive summary

Best practices of cybersecurity leaders

1. **Continuously up their game.** Because they are in an arms race with cyber criminals, CISOs need to keep their cybersecurity programs ahead of the curve. To do this, leaders spend about 25% more than others on cybersecurity per employee, increase those investments each year more than the average, and invest more in recruiting specialists, working with consultants, and training, such as end-user security awareness training with simulated phishing.
2. **Make cybersecurity hygiene a top priority.** Leaders have the lowest percentage of unpatched “critical” or “high” vulnerabilities based on CVSS scores (18% for leaders vs. 28% for others). They also do more frequent backup restoration drills (5.6 times a year vs. 4.3 for non-leaders) and IT infrastructure scans (4.9 vs. 3.8), as well as more phishing tests (5.1 vs. 4.4).
3. **Keep management teams focused and aligned.** Cybersecurity heads typically report to the CEO, COO, or the Board in leader companies. CISOs at these firms focus more on security than IT (75% of leaders) and play a bigger role in digital transformation (57%), managing data privacy (54%), and operational resiliency (49%). They are more likely to have two executives share responsibility for cybersecurity, such as the CIO and CISO, or the CISO and CSO.
4. **Rely heavily on advanced analytics and specialized teams.** More than 8 out of 10 leaders conduct cyber-risk scenario analysis, assess the financial impact of risk events, and measure the effects of mechanisms to mitigate cyber risks. Leaders also outsource incident response, red team, risk management, and security ops more often than others.
5. **Extract greater value from cybersecurity tools.** Leaders invest more in—and get greater effectiveness from—key cybersecurity technologies, including cloud workload security, endpoint detection, mobile device management, deception technology, email filtering, multi-factor authentication, and firewalls and web filtering.
6. **Make more use of cybersecurity insurance to transfer risk.** Fifty-seven percent of leaders have cyber insurance coverage over \$10 million, versus 30% of non-leaders. Overall, 60% of firms plan to spend more on insurance over the next two years.

These are the six main practices used by cybersecurity leaders to mitigate risks in today’s fast-changing, digitally enabled environment.



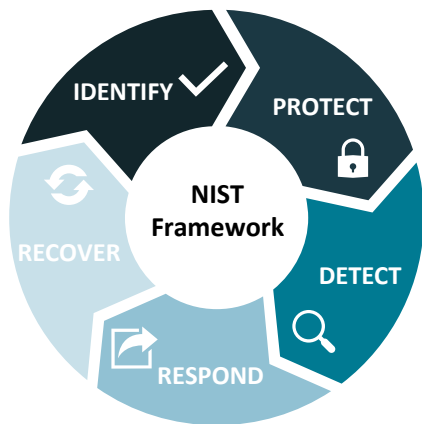
Assessing cybersecurity maturity

How we defined cybersecurity maturity

Because of the complexity of managing risks in a digitally interconnected world, creating a framework for benchmarking cybersecurity performance is complicated. Simple compliance with a security framework such as NIST, for example, does not guarantee the best results. Self-assessments of progress may lack objectivity, and externally observable data may not tell the whole story. To address these pitfalls, ESI ThoughtLab formulated a scoring framework for measuring the cybersecurity performance of the 1,009 companies in the study, using three equally weighted pillars (described on next page).

Pillar 1

Progress against the NIST framework



Pillar 2

Effectiveness in mitigating breaches and losses

Average number of attacks and breaches last year

Attempted attacks	67
Minor security incidents	23
Moderate breaches	5
Material breaches	0.06
Total breaches	28
Attempts per breach	3

Pillar 3

Verizon Business cyber risk ratings

Score overview					
Overall security posture			Threat level		
Score confidence 70%			Score confidence 50%		
Current score 550			Current score 4.0 – Very High		
Last 6 months			Last 6 months		
Low 520 High 780			Low 2.9 High 5.0		
Basic 0-600 Intermediate 600-750 Advanced 750-1000			Critical 5.0 Very high 4.0 High 3.0 Med 2.0 Low 1.0		

Our scoring methodology

For the **first pillar**, we determined a company's progress against NIST based on its self-reported score on the five NIST dimensions: identify, protect, detect, respond, and recover.

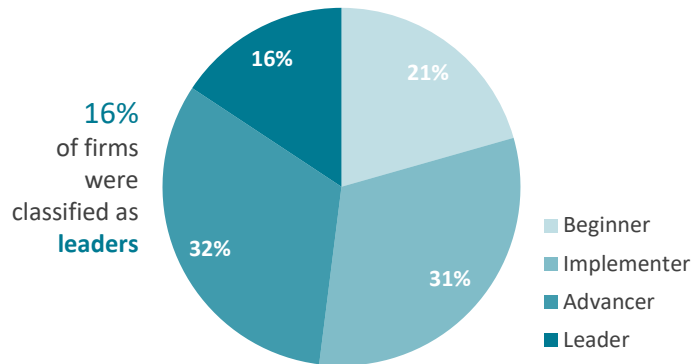
For the **second pillar**, we assessed the effectiveness in (1) preventing breaches, based on the ratio of successful breaches to attempted attacks; (2) containing the cost of a breach, based on its average cost; and (3) mitigating the cost of an attack, based on the time to identify, contain, and recover from it.

The **third pillar** is the Level 1 score (ranging from 0 to 1,000) from the Verizon Business Cyber Risk Monitoring Tool. The score provides an outside-in view of the company's cybersecurity maturity, based on publicly available data from Bitsight and the Verizon Business Data Breach Investigations report.

For each pillar, we scored companies 0 to 5 based on their performance against the criteria for that pillar. We then averaged the scores for each pillar to derive an **overall ranking** for each company. Each respondent was classified into one of four stages of cybersecurity maturity, beginner, implementer, advancer, and leader, based on that ranking.

The maturity analysis is based on 777 firms covered by both the survey and the Verizon Business ratings. Because the Verizon Business ratings penalize telecoms for the poor cybersecurity performance of their customers, we based our rankings for this sector only on progress on the NIST framework and cybersecurity effectiveness.

% of companies in each maturity category



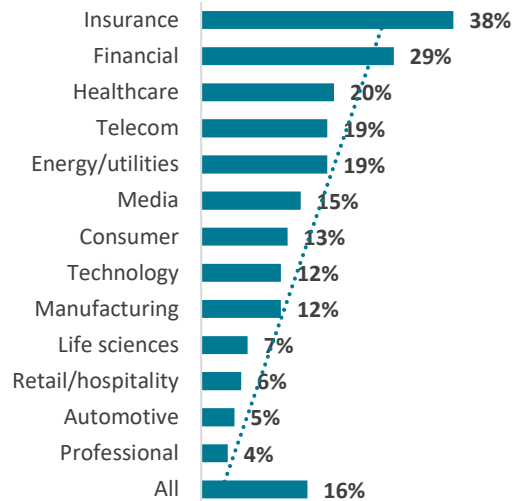
Which companies lead in cybersecurity?

Insurance, financial, and healthcare firms are the most advanced in cybersecurity, while retail, automotive, and professional service companies are the furthest behind—not a good place to be in today’s riskier business environment.

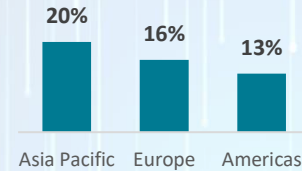
With their financial assets at stake, it is no surprise that insurance and financial firms are most ahead, followed by healthcare, which needs to protect sensitive patient data. Surprisingly, professional firms, many of which advise other companies, have the lowest share of leaders. Retail and hospitality firms, already well behind, will be hurt further as the financial fallout from the coronavirus may damage their cybersecurity budgets. Even tech companies, with their fail-fast mentality, may be cutting corners on cybersecurity. Yet the coronavirus lockdown has been a wake-up call, underscoring the need to invest further and to combine a preventative mindset with consolidated security architecture.

The larger the company, the greater its cybersecurity maturity. By region, firms in APAC tend to be more advanced, while those in the Americas—pulled down by poorer performance by those in Brazil—are doing less well. The General Data Protection Regulation (GDPR) has spurred enterprises in Europe to improve cybersecurity.

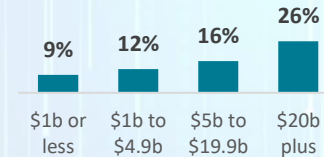
% of leaders by industry



% of leaders by region



% of leaders by revenue



“Rather than thinking of the coronavirus and stay-at-home orders as an obstacle, CISOs should see the situation as an opportunity to demonstrate our strength and capabilities. Many organizations have been able to react swiftly, change systems, and enable our enterprises to keep going. Executives have felt the importance and positive influence that the cyber security team has on day-to-day operations.”

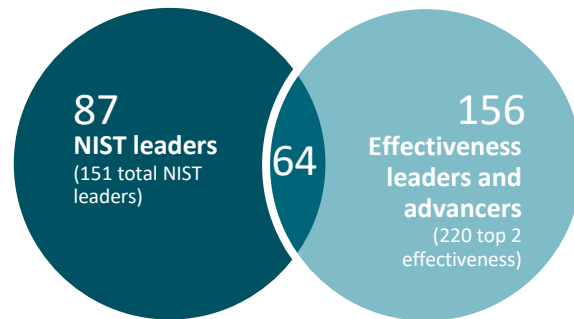
Jony Fischbein, CISO, Check Point Software

NIST compliance alone does not drive cybersecurity effectiveness

Only 64 of 151 companies (42%) classified as leaders in NIST compliance are advanced in cybersecurity effectiveness. The numbers confirm what many CISOs already know: firms need to go beyond NIST and other frameworks to secure their enterprises from escalating cyberattacks.

While NIST provides a solid foundation for cybersecurity planning, communication, and regulatory compliance, it is not enough to ensure the effectiveness of companies' cybersecurity programs. Rather than applying the NIST framework as a box-ticking exercise, the most cyber-mature companies adapt this and other frameworks to their business goals, strategies, and individual risk profiles. Cybersecurity leaders also combine analysis from advanced quantitative tools and input from internal business partners and third-party experts to make the best decisions.

Overlap between NIST leaders and companies that are effective at mitigating cybersecurity risks



“If you walk into an organization and say, we’re just going to implement NIST and ISO to manage cybersecurity, you’re going to get thrown out the door. That’s not how it works. It starts with a good understanding of the business and having a dialog with the business leaders to ensure that your cybersecurity program is aligned with their objectives. You then take the best from those frameworks to develop the appropriate approach for your organization.”

Juan Morales, Deputy CISO, Realogy





The emerging risk landscape

Malware and phishing are responsible for largest cyber losses

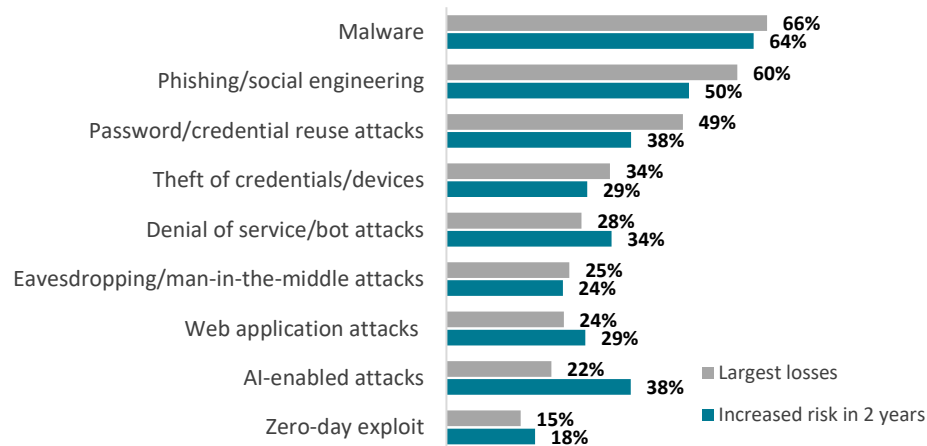
Across all industries, firms see the largest losses from malware, phishing, and password reuse. The pandemic has heightened the risk from these threats.

Even before COVID-19 hit, firms saw malware, phishing, and password reuse as the largest risks. Indeed, according to John Loveland, Global Head of Cybersecurity Strategy & Marketing at Verizon Business, credential theft and attacks via phishing and business email caused more than 67% of breaches in 2019.

But the crisis has upped the stakes, as consumers rely more on e-commerce and telemedicine, and staff on remote working—often on less-secure devices and connections. Adding to the risks, cyber criminals are ramping up malware and phishing attacks to exploit coronavirus fears.

The mounting use of technology, another by-product of the health crisis, will also take its toll. As business goes digital over the next two years, executives expect a rise in attacks through denial of service (34%) and web applications (29%). But the biggest jump in risk will come from AI-enabled attacks (38%). With its ability to learn and adapt, AI will transform cyber warfare by allowing assailants to execute more personalized and insidious attacks.

Losses and risks from attack vectors



“As attackers learn how to deploy machine learning and AI, the speed of attacks will increase immensely. These programs will enable malicious actors to automate emails that look incredibly realistic—no longer just those from a Nigerian prince filled with misspellings.”

Ron Mehring, VP Technology & Security, Texas Health Resources

Q28: Which types of attacks are causing the largest losses today and which will pose a higher risk for your business over the next two years?

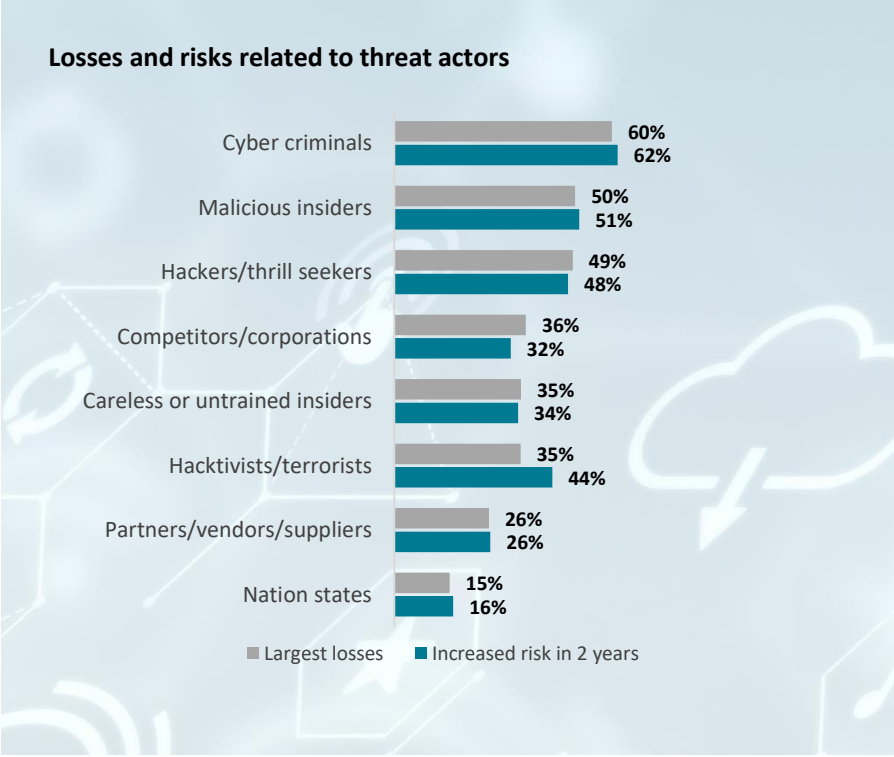
Cyber criminals will continue to cause the largest losses

While it is difficult to discern one threat actor from another, CISOs surveyed believe that cyber criminals currently inflict the biggest losses, followed by malicious insiders and hackers. CISOs expect these threat actors to continue to wreak havoc over the next two years as digital innovation accelerates.

Cyber criminals and hackers are getting better at targeting and attacking companies. And new vulnerabilities are emerging as telework expands, allowing hackers to exploit unsecured Wi-Fi and personal devices. Capitalizing on pandemic fears, criminals have impersonated public health officials, medical experts, and senior executives to get users to click malicious links. Ransomware attacks on critical infrastructure are another growing area of concern.

Malicious insiders cause some of largest losses and will pose even greater risks in two years. Insider attacks may rise as employees become disgruntled owing to layoffs during the pandemic. Careless and untrained staff—the top threat in our 2018 study—are under better control due to company-wide training programs. CISOs report smaller losses from those sources. But this could change as telework creates more room for mistakes.

While partners and suppliers are not cited as a top risk now, this too could shift as COVID-19 has severely disrupted supply chains. Third-party due diligence is becoming a higher priority as the pandemic causes greater supply chain vulnerabilities.



Q29: Which internal or external threat actors are causing the largest losses today and which will pose a higher risk for your business over the next two years?

Hacktivists and nation-states loom as rising threats

Companies see hackers as one of the fastest-growing risks over the next two years. With geopolitical and social unrest bubbling, CISOs are bracing for a rise in cyber terrorism and activism. The pandemic is stirring the pot by triggering greater economic instability and new tensions between the US and China and throughout the EU.

With deep pockets, sophisticated cyber techniques, and a unique ability to cover their tracks, nation-states are a nagging worry for CISOs. They pose a growing threat to many industries, particularly retail and hospitality, automotive, financial, energy, and life sciences. The motives behind attacks range from stealing sensitive customer data and financial assets to competitive espionage and intellectual property theft.

COVID-19 has exposed organizations to a rash of new attacks. During the peak of the crisis, the US Health and Human Services Department was hit by a denial of service attack to impede its response. In May, the US FBI warned of Chinese hackers trying to steal research data on coronavirus vaccines, and Israel accused Iran of attempting to cripple water supplies during the pandemic.

% seeing largest increase in risk from nation-states

	Now	Two years	Increase
Retail/hospitality	10%	21%	11%
Automotive	14%	22%	8%
Financial	14%	22%	8%
Energy/utilities	13%	18%	5%
Life sciences	17%	21%	4%
Telecom	14%	17%	3%
Insurance	13%	16%	3%
Technology	14%	16%	2%

“Companies are in the crosshairs of nations and their motivations. We learned from US officials that the data breaches of Equifax and the Office of Personnel Management came from the Chinese government. The hard question is, how can a company marshal enough resources to stop one of the largest and most powerful governments in the world from getting into your systems? That seems like a daunting and almost impossible task for most companies.”

Joe Sullivan, CISO, Cloudflare

“Financial services firms encounter numerous technology-based attacks. Nation-state attacks are sophisticated and difficult to detect. The motivation for these attacks is not simply financial. They want persistent access to the financial services infrastructure to use when needed.”

Jason Harrell, Executive Director, Technology Risk Management, DTCC

Q29: Which internal or external threat actors are causing the largest losses today and which will pose a higher risk for your business over the next two years?

Remote working, connected devices generate greater risks

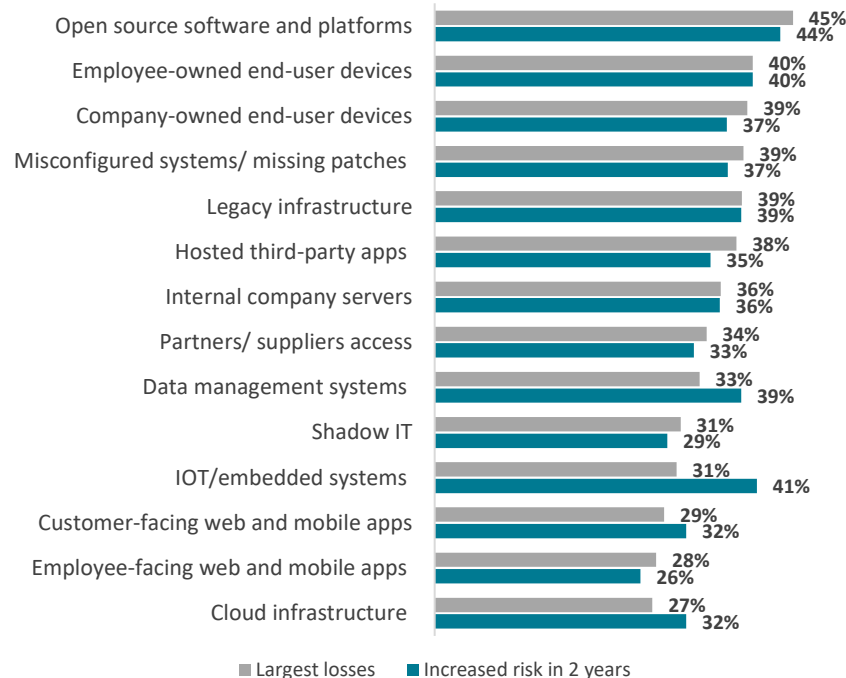
As firms embrace open-source platforms and telework, they become exposed to greater cyber risks. These may rise beyond expectations as the pandemic shifts more work to home offices and healthcare to smart devices.

Open-source platforms generate the largest losses for most companies now and will pose the greatest risks in two years. The massive Equifax breach in 2017, related to a vulnerability in Apache Struts, an open-source web application, underscored the dangers of open-source software. CISOs also see employee- and company-owned end-user devices as major drivers of risk. During the pandemic, they have had to devise strategies to secure home PCs and mobile phones used to access network servers.

These vulnerabilities vary considerably by industry. Financial service companies are experiencing the largest losses and expect the biggest future risks from legacy infrastructure. For manufacturing, misconfigured systems pose the greatest danger; for media and entertainment, it is third-party applications.

Emerging technology will multiply the risks. For example, 41% of respondents say IoT and connected devices will pose the biggest risk in two years, up from 31% today. That is partly because the rollout of 5G is expected to boost the number of connected devices. Data and analytics, customer-facing web and mobile applications, and cloud infrastructure also are expected to heighten cyber risks over the next two years.

Losses and risks from vulnerabilities



Q30: In which areas of your IT infrastructure are cyberattacks causing the largest losses today and which will pose the largest risk in two years?



Organizing for cybersecurity success

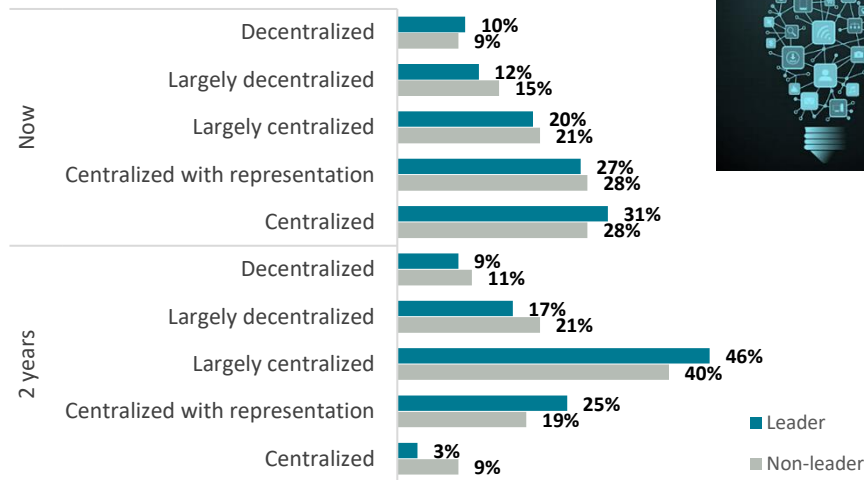
Leaders are moving to shared cybersecurity control

As firms digitally transform, their business divisions often assume responsibility for digital operations. In response, cybersecurity functions are moving away from rigid centralization to central teams sharing budget and staff with other departments.

Most companies, particularly cybersecurity leaders, are transitioning to hybrid forms of centralization, or even decentralization. But these shifts, while often necessary because of the size or underlying organization of the firm, can be challenging to orchestrate while maintaining control. That is why over a quarter of firms will remain centralized for security.

To make shared responsibility work, firms need proactive central cybersecurity teams to provide valuable cybersecurity oversight, frameworks, processes, and technologies. CISOs find that advanced data management systems that provide rapid information to governance teams can help ensure cybersecurity success.

Cybersecurity organization type, %



Cybersecurity organization types

Centralized: all (or nearly all) cybersecurity staff and budget reside in a central department(s).

Centralized but with representation from various departments, such as IT or legal.

Largely centralized: central department(s) with some staff and budget in business units.

Largely decentralized: staff and budgets reside in business units, with some in central department(s).

Decentralized: all (or nearly all) cybersecurity staff and budgets in business units.

Q13: Which best describes how your company is now organized for cybersecurity? Which best describes your approach over the next two years?

Finding the right calibration of control for your business

The case for staying centralized



"My team has been most effective in a centralized setting. My primary role is to be the executive voice—to ensure that security is calibrated correctly and that the risks get resourced and addressed properly. Without executive judgment, security teams can be focused on the wrong risks. You need someone to make sure that resources are aimed at the most important places. I don't know how that gets done well in a decentralized world."

Joe Sullivan, CSO, Cloudflare



"When I worked at a large, decentralized organization where CISOs were in every business unit it was very dysfunctional, and it was difficult to get all business units to align. Here, we centralized the entire security organization. That has been one of the keys to our success."

Juan Morales, Deputy CISO, Realogy

The case for moving to shared control



"Our IT and security have for years been very centralized, but that's changing. Business leaders are becoming more tech savvy and are assuming more responsibility for their technology stacks. The security team needs to adapt to that shared control. We've done that by establishing a control allocation model, assigning specific responsibilities to executive-level stakeholders in the business units. That way, we clearly understand the lines of authority and who owns the risk."

Ron Mehring, VP Technology & Security, Texas Health Resources



"You have to make cybersecurity scalable, because cybersecurity is not one person's job. It's everybody's job. The central teams need to decentralize areas of cybersecurity. The people that you hire in cybersecurity need to be able to take their knowledge and evangelize cybersecurity to all the other teams in the enterprise, to make it more scalable."

Chintan Jain, Founder & VP of Security Engineering, Security Mantra

Case Study

How Teva Pharmaceuticals ensures cybersecurity control



Ilan Abadi,
Global CISO, Teva
Pharmaceuticals

With 43,000 employees, 10,000 vendors, and a far-flung global footprint, Teva Pharmaceuticals needed to develop a cybersecurity approach that blends central control with decentralized implementation. According to Ilan Abadi, the Global CISO, “If you centralize everything, it will be much more difficult for a large enterprise like ours located in more than 60 countries.”

To oversee the firm’s cybersecurity program, Abadi built a small, agile team of about 35 people at the center and a few professional cyber personnel at central business hubs worldwide. The team includes three functional groups. The first is an expert team responsible for infrastructure, networking, cloud, apps, and other cybersecurity activities. The second is the GRC team that is responsible for audit, risk management, and active technical governance. The third is the 24/7 Cyber Defense Center with tier 1, 2, and 3 analysts. The cybersecurity team also draws as needed on specialists from outside the company.

Blending central control with decentralized responsibility

The central cybersecurity team trains and empowers the 1,200 people in Teva’s worldwide IT department, who share responsibility for managing cybersecurity. To stay on top of risks, the central team uses a digitally enabled governance platform that scans, audits, and tests (BAS) networks and devices regularly. It also employs a data lake that runs analytic searches for potential and real-time threats. “Active governance can give you what you need to know when you need to know it,” says Abadi.

Abadi has established a robust set of compensation controls connected to the governance and Cyber Defense Center. Whenever one of these controls goes down, a ticket automatically goes to the governance team. His central team has also built a cybersecurity framework and guidance procedures that are used by the various IT groups, such as developers, finance IT, and commercial IT. In that way, Abadi can ensure the best cybersecurity practices across the enterprise.

Given the turnover among cybersecurity staff, Abadi has learned over his 20 years of experience the vital importance of maintaining a time-tested cybersecurity playbook that spells out policies, procedures, and guidelines for all staff. It also helps the team manage black swan events, like the pandemic. “I learned this when I was in the armed forces. It’s all about having the right crisis management process in place to enable your team to make very fast decisions both before and after the boom.”

Leaders typically assign dual responsibility for cybersecurity

To integrate cybersecurity across their businesses, more than three-quarters of leaders have two executives sharing responsibility. These most often are the CIO and CISO, but other combinations include the CIO-CTO, CISO-CSO, and CIO-CSO.

The greater a company’s size, the more likely it will create a dual structure. For example, 85% of enterprises with revenue over \$20 billion divide responsibility for cybersecurity between two executives, compared with just 24% of companies with revenue under \$1 billion. When there is just one executive in charge, it is usually the CIO or CISO. At 52% of leader companies, the CIO is in charge.

1 2 How many in charge

	Leader	Non-leader
<div>Single</div>	19%	34%
<div>Two</div>	76%	49%

💰 How revenue size affects role

	Up to \$1b	\$1b-\$4.9b	\$5b-\$19.9b	\$20b +
<div>CISO*</div>	11%	30%	49%	60%
<div>Shared</div>	24%	44%	60%	85%

* When only one executive in charge, the percentage of times that person is a CISO

👤 Single executive in charge

	Leader	Non-leader
CIO	52%	34%
CISO	30%	35%
CTO	13%	18%
CDO	4%	3%
CSO	0%	4%
CRO	0%	3%
CPO/CDPO	0%	1%

👥 Two executives in charge

	Leader	Non-leader
CIO/CISO	30%	23%
CIO/CTO	23%	17%
CIO/CSO	8%	8%
CISO/CSO	5%	10%
CIO/CDPO	4%	5%
CISO/CRO	3%	6%
CISO/CTO	3%	6%

Q12: Which best describes how responsibilities to oversee cybersecurity are assigned at your company? Q12a and b: Which of the following reflects their title/titles?

Cybersecurity reports to top management, especially among leaders

Most executives in charge of cybersecurity report to the CEO, while only about 2 out of 10 report to the CIO. For over three-quarters of leaders, cybersecurity reports into top management, either to the CEO, COO, CFO, or the Board.

Cybersecurity is most effective when it is part of the corporate strategy and treated as a critical business function, not just a function of IT or risk. That is why most companies, not just leaders, now have their cybersecurity heads report directly to the CEO. When given a seat at the table, cybersecurity directors can better understand and support the strategic objectives across the organization. Direct access to the CEO also ensures cybersecurity issues are addressed quickly and effectively.

Many CISOs still report to the CIO, but companies are questioning the wisdom of this approach. Says the CISO of one financial services firm: “If your CISO reports to the CIO and has operational responsibilities, you don’t have a CISO, you have an operations person who does a little security. The cybersecurity group must have objectivity and the independence to be able to state its opinion.”

“I report directly to our CEO because we believe that the security function should be independent from other business units. That way, when things are detected as a high-priority security event, I can go straight to the CEO.”

Brian Jack, CISO, KnowBe4

Cybersecurity reports to:	Leader	Non-leader
Top management		
CEO	63%	61%
COO	6%	0%
Board/board member	5%	4%
CFO	2%	0%
Other C-Suite		
CIO	17%	21%
Chief Risk Officer	4%	1%
CISO	2%	2%
CTO	1%	7%



Q12c: To whom do[es] the executive[s] responsible for cybersecurity directly report?

Cybersecurity leaders give CISOs a bigger business role

CISOs are expanding their role as they sharpen their focus on security over IT and play a bigger part in digital transformation, data privacy, and operational resiliency. Leaders are paving the way.

Within three quarters of cybersecurity leaders, the role of the CISO is moving from a generalized IT role to that of a specialized cyber risk manager—a technology-savvy professional working with stakeholders around the firm to build security and resiliency into their business processes.

As firms become leaders, their CISOs typically share more responsibility for digital transformation and data privacy. They also often become more involved in diverse business areas—from operational resiliency and product development to supply chain management, and even geopolitical risk management.

With regulatory and social pressures building, companies are combining data security and privacy into one role or closely entwined roles. According to Juan Morales, Deputy CISO of Realogy: “The more consumer data out there, the more we need to protect it. Data privacy and security go hand in hand.”

Changes in CISO role	Leader	All others
Greater focus on security than IT	75%	68%
Bigger role in digital and business strategy	57%	45%
Expanding data privacy and compliance responsibilities	54%	42%
Greater involvement in operational resiliency	49%	41%
Increasing interaction with board/senior management	38%	32%
Partnering more with other functions, departments	36%	31%
More analytical driven in approach	30%	31%
Greater engagement in product development	30%	26%
Wider role in enterprise, geopolitical risk management	26%	25%
Bigger part in third-party/supply chain management	22%	21%
Higher stature, visibility, and managerial responsibility	18%	23%

“The CISO’s responsibilities are being expanded to support resilience. CISOs must have a deeper understanding of a business’s operations, business model, and risks so that the proper set of controls can be applied that enhance the business’s resilience to technology-based attacks.”

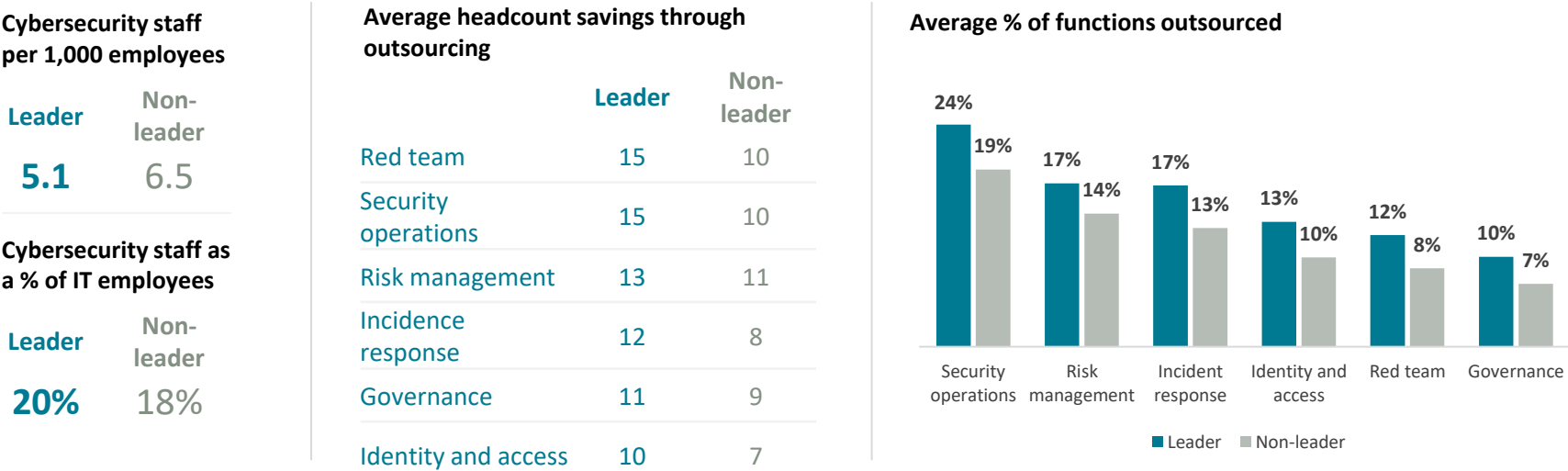
Jason Harrell, Executive Director, Technology Risk Management, DTCC

Q16: What, if any, are the ways that the role of the CISO is changing at your company?

Leaders rely on outsourcing to access skills and build resilience

Leaders save on cybersecurity staff headcount by making better use of IT staff and outsourcing more specialized functions.

Leaders have fewer cybersecurity staff as a share of total employees than non-leaders but make better use of internal IT staff. One reason they run leaner is that they typically outsource more cybersecurity operations, particularly security, risk management, and incidence response. These functions often require cybersecurity skills that are hard to develop or acquire. Outsourcing also can ensure continuity, since these specialists can be difficult to retain.



Q14: Not counting staff within outsourced functions, how many internal and external full-time equivalent staff does your company hire to manage cybersecurity?
 Q15: What % of the following cybersecurity functions do you outsource and what were the headcount savings?

How to use outsourcing to drive better cybersecurity results



"The security organization is in a constant state of evolution and evaluation. Some of the evaluation work, you can outsource for efficiency. We're seeing third-party vendor analysis being outsourced. We're seeing more of the compliance certification auditing being outsourced. We see a lot of outsourcing happening around managed services."

Joe Sullivan, CSO, Cloudflare



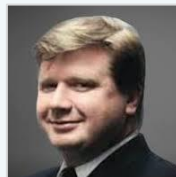
"Outsourcing is becoming the norm. Going forward, we're going to use a blend of managed services where we know we have talent acquisition challenges as well as retention. That way, if you have churn of talent, you know the engine's going to keep on running. However, you want to make sure a managed services team is a good fit culturally, otherwise you end up having friction between different engineering teams."

Ron Mehring, VP Technology & Security, Texas Health Resources



"We bring in managed service or security partners to help us on two ends of a continuum. At one end, it's commodity, repeatable, 24/7-type activities. Those can be easily outsourced. On the other end are boutique, never-seen-before activities, where someone shows up with a gigantic set of tools and the expertise to operate them."

Jeffrey Coe, CISO, ON Semiconductor



"Before you use third parties, you need to clean your own house. Looking for a third party to put your house in order doesn't work well. If you set up your internal operation right, you can share information with any MSP. They can provide additional value by telling you the things you need to do."

Richard Rushing, CISO, Motorola Mobility



Investing effectively in cybersecurity














Leaders spend more to ensure cybersecurity excellence

On average, firms spent \$9.6 million last year on cybersecurity, about \$515 per employee. Leaders spent far more—\$15 million, or \$618 per person.

In general, as companies move up the cybersecurity maturity curve, they spend more on cybersecurity. Leaders spend twice as much as beginners on cybersecurity on an absolute basis and about 30% more per employee. Larger firms also spend more on cybersecurity, both in absolute terms and by employee.

Insurance, energy/utilities, and automotive spend the most on an absolute basis, while media and entertainment, professional, and healthcare spend the least. But the picture shifts when spending is measured per employee: energy/utilities and insurance stay the largest, but labor-intensive sectors, like automotive and manufacturing, fall to the bottom.

Current total spending on cybersecurity

	Total \$M	Per employee
 Insurance	\$15.55	\$1,077
 Energy/utilities	\$12.89	\$1,110
 Automotive	\$12.74	\$ 265
 Telecom	\$11.12	\$ 452
 Financial	\$11.03	\$ 516
 Life sciences	\$10.76	\$ 471
 Retail	\$10.12	\$ 474
 Consumer	\$ 8.81	\$ 403
 Technology	\$ 8.40	\$ 364
 Manufacturing	\$ 7.44	\$ 313
 Healthcare	\$ 6.48	\$ 404
 Professional	\$ 4.91	\$ 329
 Media	\$ 4.17	\$ 516

By company revenue size

	Up to \$1b	\$1b- \$4.9b	\$5b-\$19.9b	\$20b+
Total in \$M	\$0.71	\$2.53	\$9.29	\$29.16
Per employee	\$427	\$444	\$560	\$626

By cybersecurity maturity

	Beginner	Implementer	Advancer	Leader	All
Total in \$M	\$7.50	\$9.29	\$11.49	\$15.08	\$9.58
Per employee	\$473	\$430	\$561	\$618	\$515

*All includes some respondents not classified by maturity

“While technology and preventive investments remain a staple of security budgets, more firms are recognizing the need to round out their control portfolios with administrative and physical controls across different functions such as detective, corrective, deterrent, recovery, and compensation.”

Brian Wrozek, VP, Corporate Security, Risk & Compliance Management & Physical Security, Optiv

Q17: What is your company’s current total cybersecurity spending—the full amount that your company currently spends on people, process, and technologies for managing cybersecurity, including ongoing and one-off project costs?

Leaders plan to boost cybersecurity spending more

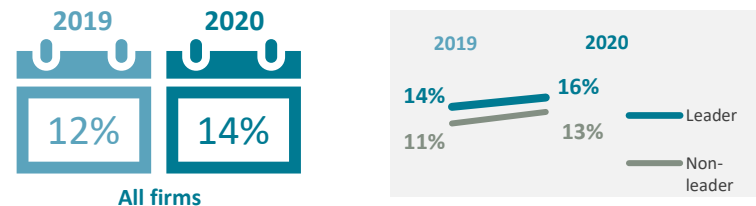
During 2020, 97% of firms expect to hike their spending, on average by 14%. Leaders plan increases of 16%. But the pandemic may alter their plans.

Cybersecurity spending has been climbing with growing digital use. In 2019, companies increased spending by 12% on average. Leaders hiked spending even more—by 14%, as did financial service firms and companies with revenue over \$20 billion.

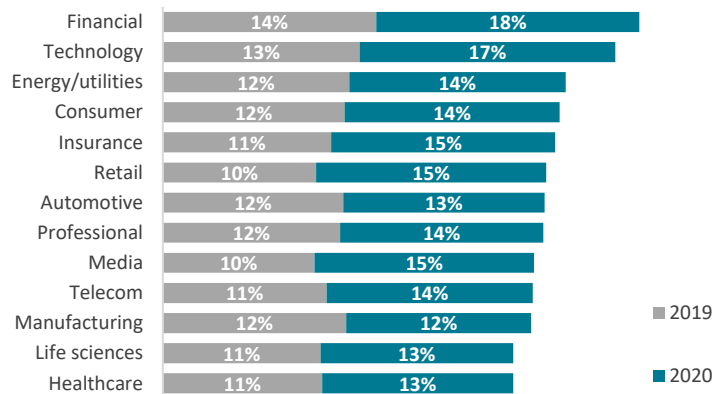
All industries in our survey expect to boost their spending in 2020 by more than they did in the prior year, except for manufacturing. For some sectors, the planned increases are ambitious: 18% for financial services, 17% for technology, and 15% for insurance, retail, and hospitality.

However, COVID-19 likely will affect cybersecurity spending in the months ahead. Our interviews during the pandemic show a divergence of views, with some companies, particularly those in hard-hit areas like retail and hospitality, expecting significant budget cuts, and others foreseeing increases to support more ambitious digital transformation plans. The depth and length of the economic downturn will be a determining factor.

Average increase in cybersecurity spending



Average increase in cybersecurity spending by industry



Q18: How much, if at all, did your company’s cybersecurity budget increase over the last year and how much do you expect it to increase in the future?

Where companies are investing their cybersecurity dollars

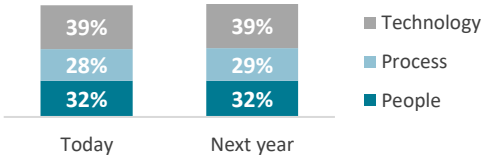
Regardless of their cybersecurity maturity, size, and industry, firms invest the most in technology, followed by people and process. They expect these allocations to stay roughly the same in 2020.

Allocations vary by industry. Automotive and manufacturing earmark more than average for people (34%) and less than average for technology (37%). Financial services, telecom, and life sciences do the reverse: they allocate less for people (31%) and more for tech (41%). Most CISOs treat this holistically, blending people, process, and technology investments to achieve their cybersecurity objectives.

Over 2020, the 1,009 companies surveyed plan to spend \$3.5 billion on people, \$3.1 billion on improving processes, and \$4.3 billion on technologies. However, CISOs may need to adjust budgets due to the impact of the pandemic. For example, Juan Morales, Deputy CISO of Realogy, expects his budget to remain flat or even shrink because of a fall in real estate transactions. As a result, he foresees decreased spending on hiring and training.

But spending cuts may cause further problems for some companies, says Chintan Jain, VP of Security Engineering at Security Mantra. “Many firms are already short on cybersecurity staff, so if they cut more, they are going to expose themselves to increased risks.”

% of spending on different areas*



*May not sum to 100 due to rounding

“The right balance between people, process, and technology is the hallmark of a highly successful and resilient cybersecurity program.”

Mike Convertino, CSO, Arceo.ai

Allocation by:	Automotive	Consumer	Energy	Financial	Healthcare	Insurance	Life sciences	Manufacturing	Media	Professional	Retail	Technology	Telecom
People	34%	33%	32%	31%	32%	32%	31%	34%	33%	33%	33%	32%	31%
Process	29%	28%	28%	28%	28%	29%	28%	28%	29%	29%	28%	29%	27%
Technology	37%	39%	40%	41%	40%	39%	41%	37%	38%	38%	38%	39%	41%

Q19: What percentage of your cybersecurity budget is devoted to people, process, and technology, and the five key NIST cybersecurity areas?

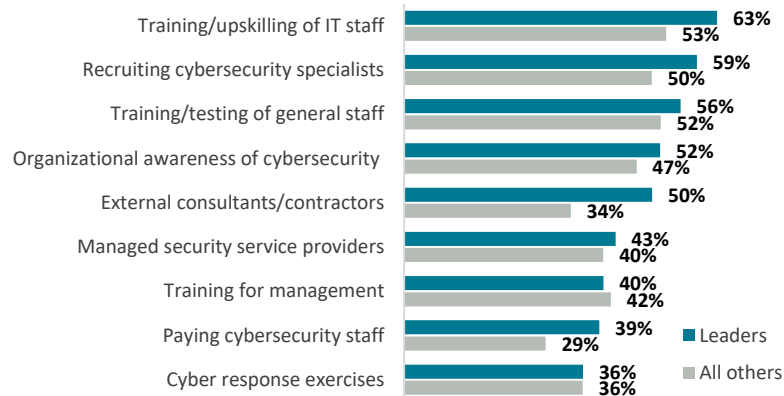
Investment in people is paying off for leaders

Leaders tend to invest more in skills, training, and resources required to excel at cybersecurity.

Leaders are more likely to make large investments in training and upskilling IT staff, recruiting cybersecurity specialists, and compensating cybersecurity staff. The biggest gap with other firms is spending on external consultants and contractors—half of leaders make big investments in this area vs. about a third of less-mature firms.

Energy and utility firms lead the pack in recruiting specialists, while consumer companies focus more than others on training and upskilling IT staff. The financial sector makes the largest investments in periodic cyber-response exercises, while automotive makes the biggest investments in training general staff and top management.

% of companies making large investments



Where industries lead

⚡ Energy/utilities

68% Recruiting specialists
46% Managed security service providers

🛒 Consumer

65% Training and upskilling IT staff
37% Compensating cybersecurity staff

🚗 Automotive

63% Training and testing general staff
53% Preparedness training of top management

💻 Technology

54% Ensuring organizational understanding of cybersecurity

🏦 Financial

46% Periodic cyber-response exercises
37% Compensating cybersecurity staff

🏭 Manufacturing

46% Managed security service providers

📶 Telecom

46% Managed security service providers

🏠 Insurance

45% Working with external consultants and contractors

Q20: Of your current cybersecurity budget for people, in which of the following security measures are you making the largest investment, and how effective have these larger investments been in reducing risks?

Which people investments are most effective?

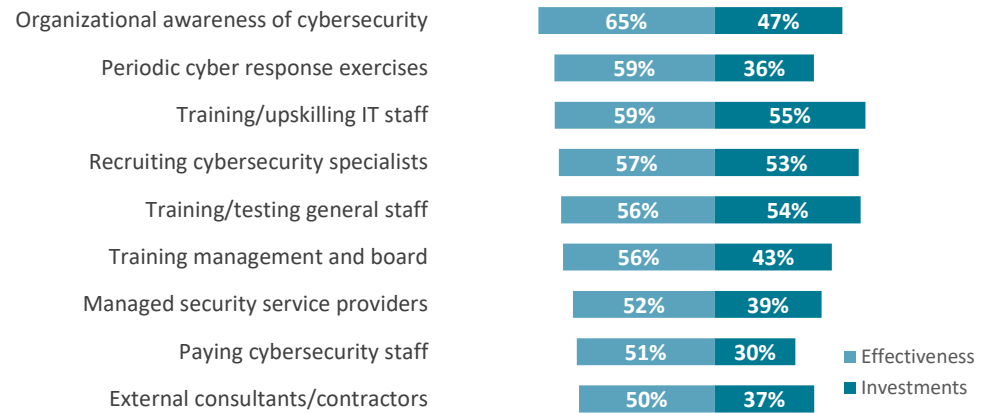
Investing in resources and training is a key plank of any successful cybersecurity strategy. When investing in people, firms should consider the areas that are most effective in reducing risks.

Our research reveals that the three most effective people areas are ensuring awareness of cybersecurity, undertaking periodic cyber-response exercises, and training IT staff. Companies also report strong results from recruiting cybersecurity specialists and training the general staff and top management.

Yet companies may be underinvesting in some of these areas, such as cyber-response exercises and training top management. Other missed opportunities, depending on the industry, include working with managed service providers, providing the right compensation for cybersecurity staff, and working with external consultants.

Looking at the approach of leaders offers additional insights. First, it highlights an area of general underinvestment that leaders find effective: using external consultants and contractors. Second, it demonstrates the ability of leaders to extract greater value from training—a strength that has served companies well during a time of remote working.

% of firms making large investments and finding them effective



Effectiveness	Leader	Non-leader	Value gap
Training/testing general staff	78%	52%	26%
Training/upskilling of IT staff	75%	55%	20%
Organizational awareness of cybersecurity	75%	62%	13%
Recruiting cybersecurity specialists	67%	54%	13%
External consultants and contractors	66%	47%	19%

Q20: Of your current cybersecurity budget for people, in which of the following security measures are you making the largest investment, and how effective have these larger investments been in reducing risks?

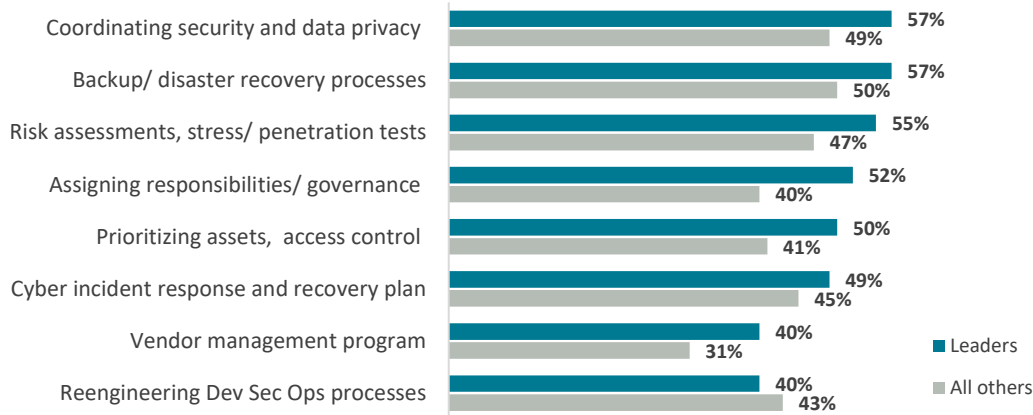
Leaders also make bigger investments in process

Cybersecurity leaders outstrip other firms in making investments in nearly all process areas. For these advanced organizations, process provides the foundation for proper control.

Cybersecurity leaders understand the vital role of processes and procedures, especially when distributing cybersecurity responsibility across their enterprises. Leaders are well ahead in coordinating data security and privacy, handling backups and disaster recovery, conducting risk assessment and penetration testing, and setting out duties and governance practices.

The pandemic has highlighted the value of effective processes during times of disruption. The companies that have been most successful in weathering the crisis had well-understood business continuity plans that considered the potential impact of cascading cybersecurity risks. They also had cybersecurity playbooks that enabled internal staff and external partners and suppliers to make the right cybersecurity decisions on their own.

% making largest investments



“You can’t assume that once you teach people a process it will magically stick. You need a high-quality control program that rotates around those critical processes, and you need to review the data from that program in detail. Most of the time, faults happen in areas where we had controls or processes that failed.”

Ron Mehring, VP Technology & Security, Texas Health Resources

Q21: Of your current cybersecurity budget for process, in which of the following security measures are you making the largest investments, and how effective have these larger investments been in reducing risks?

Which process investments are most effective?

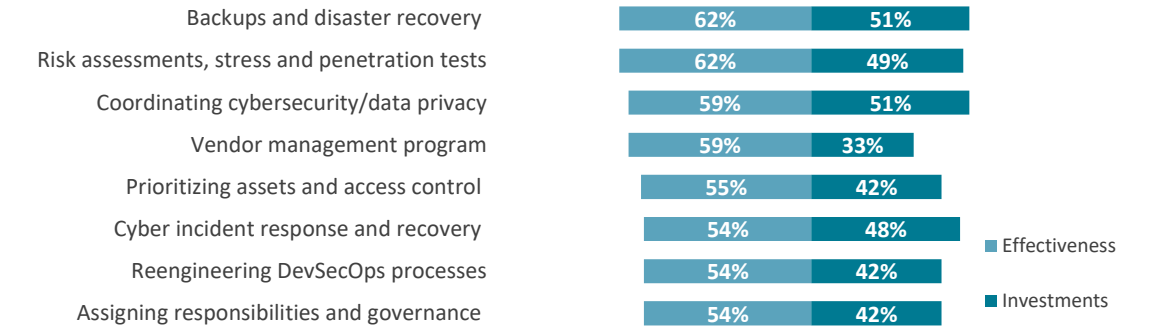
Risk assessments and stress tests, along with backups and disaster recovery, are the most effective investments—and among the most pertinent today. But only about half of firms are investing substantially in these areas.

Another process that companies should focus more on is vendor management. Only 33% of firms invest in this process area, but 59% report that it can be highly or very highly effective at reducing risk.

Companies should also consider investing more in prioritizing their assets and access control, the most effective process for leaders. Securing the assets that matter most will become even more important as company budgets come under pressure from the economic downturn.

Finally, the effectiveness gap between leaders and others in key process areas spotlights where CISOs may want to focus their efforts.

% making large investments and finding them highly effective



% finding process investments highly effective

	Leader	Non-leader	Gap
Prioritizing assets and creating access controls	72%	51%	21%
Maintaining a cyber incident response and recovery plan	68%	50%	18%
Coordinating data security and privacy	68%	58%	10%
Setting out responsibilities and governance practices	61%	51%	10%
Regular risk assessments, audits, stress and penetration tests.	67%	60%	7%
Developing and implementing a vendor management program	59%	57%	2%
Maintaining and testing of backups and disaster recovery assets	59%	62%	-3%
Reengineering processes to support Dev Sec Ops	49%	54%	-5%

Q21: Of your current cybersecurity budget for process, in which of the following security measures are you making the largest investment, and how effective have these larger investments been in reducing risks?

The pandemic is stress-testing cybersecurity processes

The rise of digital interaction and remote working along with supply chain disruption during the health crisis have exposed the weaknesses of cybersecurity processes in many firms.

Some companies were less prepared for COVID-19 because of their smaller investments in disaster recovery, response, and recovery plans, as well as risk assessments and stress-testing. Media and professional service firms trail in disaster recovery investments. Professional firms are also behind in response and recovery, as are manufacturers and technology firms, which often follow a fail-fast mentality.

It is no wonder that smaller firms, with tighter budgets, are investing less than larger ones. For example, only 42% of companies with under \$1 billion in revenue are investing substantially in disaster recovery, while 63% of those with over \$20 billion are doing so.

According to Chintan Jain, VP of Security Engineering at Security Mantra, most firms concentrate first on physical disaster recovery and then turn their attention to cybersecurity. “Many companies are still just trying to catch up and create those first systems. Then they don’t have the dollars to properly do the disaster recovery for cybersecurity systems.”



% making large investments

	Disaster recovery processes	Incident response and recovery plan	Regular risk assessments and stress tests
Automotive	55%	53%	54%
Consumer	64%	54%	54%
Energy/utilities	54%	47%	52%
Financial	55%	55%	51%
Healthcare	47%	47%	48%
Insurance	55%	60%	49%
Life sciences	58%	55%	47%
Manufacturing	52%	33%	48%
Media	39%	43%	50%
Professional	36%	39%	47%
Retail/hospitality	44%	48%	47%
Technology	52%	38%	51%
Telecom	54%	49%	45%

Q21: Of your current cybersecurity budget for process, in which of the following security measures are you making the largest investment, and how effective have these larger investments been in reducing risks?

Leaders likewise outstrip others in technology investment

Leaders invest more in cybersecurity technologies, focusing on data protection, firewalls, and email filtering and monitoring.

Many such essential technologies are preventative in nature and underscore the benefits of a prevention-first strategy. Leaders outspend others in many technologies, particularly denial-of-service mitigation, unified security architecture, email monitoring, deception technology, and multi-factor authentication.

Juan Morales, Deputy CISO of Realogy, cites five key tools that his organization relies on: a data aggregation and protection platform; a vulnerability management tool; an endpoint protection system; an AI-enabled intrusion detection system; and, to tie it together, a security orchestration and automation system. “These tools augment our staff’s ability to execute on data-driven actions,” he says.

Regrettably, firms are underinvesting in technologies crucial for telework. These include multi-factor authentication, disaster recovery, user behavior analytics, identity governance, and privileged access. Leaders are doing better in some areas, but in most, less than a third of firms are investing significantly.

“The future lies in preventing threats, simplifying security, consolidating it, and making it affordable from a resource allocation standpoint.”

Chris Scanlan, President of Americas, Check Point Software

Tech investment area	Leader	Non-leader	Difference
Data protection	59%	59%	0%
Firewalls and web filtering	55%	48%	7%
Email filtering and monitoring	48%	37%	11%
Deception technology	42%	31%	11%
Endpoint detection and protection	39%	31%	8%
Multi-factor authentication*	38%	28%	10%
Disaster recovery*	36%	41%	-5%
Network traffic analysis	34%	32%	2%
Denial-of-service mitigation	33%	19%	14%
User behavior analytics*	32%	23%	9%
Intrusion detection and protection	31%	29%	2%
Identity governance*	28%	28%	0%
Cloud workload (IaaS, PaaS) security	27%	21%	6%
Cloud-access security broker (CASB)	25%	19%	6%
Privileged access management*	25%	23%	2%
Security orchestration and automation	25%	18%	7%
Encryption and tokenization	24%	18%	6%
Unified security architecture	24%	12%	12%

* Technologies crucial for remote working

Q22: Of your current cybersecurity budget for technology, in which of the following security measures are you making the largest investments, and how effective have these larger investments been in reducing risk?

Which technology investments are most effective?

When deciding where to invest, CISOs should look to technologies that leaders find most effective.

Leaders are getting much more out of these security technologies than most firms, particularly endpoint detection, deception technology, cloud workload security, and privileged access management. Only in the case of data protection is the difference with non-leaders small.

However, some of the most effective technologies for leaders, including security orchestration, cloud security, mobile device management, privileged access management, and encryption, are areas where only about 1 in 5 firms are investing.

CISOs particularly cite the benefits of endpoint technology and AI-driven security orchestration—which can update rules and act in real time based on machine analysis. Investing in automated systems that take some of the decision-making away from the end user will help to protect the enterprise where hackers typically attack most.

Most effective cybersecurity technology investments

	Leader	Non-leader	Difference
Endpoint detection and protection	83%	59%	24%
Deception technology	82%	59%	23%
Data protection	75%	71%	4%
Security orchestration and automation*	71%	53%	18%
Cloud workload (IaaS, PaaS) security*	70%	46%	24%
Email filtering and monitoring software	69%	57%	12%
Firewalls and web filtering	69%	51%	18%
Mobile device management*	68%	56%	12%
Privileged access management*	68%	48%	20%
Encryption and tokenization*	66%	55%	11%

* Technology areas where only 1 in 5 firms are investing significantly

“It’s like a battle. If you want to win, you need the tools to read your opponent.”

Ilan Abadi, Global CISO, Teva Pharmaceuticals

“Endpoint solutions are among the technologies that make a difference. Knowing what’s going on at the endpoints provides a wealth of information that you can’t normally get from just logs.”

Richard Rushing, CISO, Motorola Mobility

Q22: Of your current cybersecurity budget for technology, in which of the following security measures are you making the largest investments, and how effective have these larger investments been in reducing risk?



Cybersecurity incidents and breaches

Attacks and breaches vary by industry

Some industries are attacked more often than others—particularly those that hold financial assets or valuable customer data, such as insurance, financial services, and retail/hospitality.

Some also do a better job of playing defense. Manufacturing, automotive, and life sciences firms perform better at keeping attempts from turning into successful attacks than professional service, financial, and retail/hospitality firms.

Less than 1% (75) of the 28,100 successful breaches suffered by the 1,009 survey respondents were material breaches. While few, material breaches generate the largest losses. Financial, retail/hospitality, and automotive firms suffer a disproportionate number of material breaches.

Financial and retail/hospitality firms suffer from the trifecta of an above-average number of attacks, above-average attempts per breach, and an above-average material breaches—but for different reasons. For financial service firms, it is “because that’s where the money is,” as bank robber Willy Sutton once said. But for retail/hospitality firms, it results more from lower maturity in cybersecurity.

“No organization is immune to cyberattacks. Industries like healthcare, retail, or financial services have been systematically targeted because they process sensitive data that have monetary value on the dark web.”

Jack Kudale, Founder and CEO, Cowbell Cyber

Reported incidents last year

	Attempted attacks	Attempts per breach*	Material breaches**
Insurance	88	3.05	0.03
Financial	84	2.65	0.12
Telecom	77	2.83	0.07
Retail/hospitality	76	2.81	0.12
Life sciences	73	3.37	0.05
Technology	67	3.18	0.06
Average	67	3.03	0.06
Consumer	67	3.17	0.03
Energy/utilities	66	2.94	0.05
Manufacturing	62	3.65	0.01
Media	61	2.86	0.05
Automotive	59	3.41	0.09
Healthcare	47	2.96	0.04
Professional	47	2.53	0.05

*The fewer attempts per breach, the less effective the defense approaches.
 **Those generating a substantial loss and requiring disclosure to a third party.

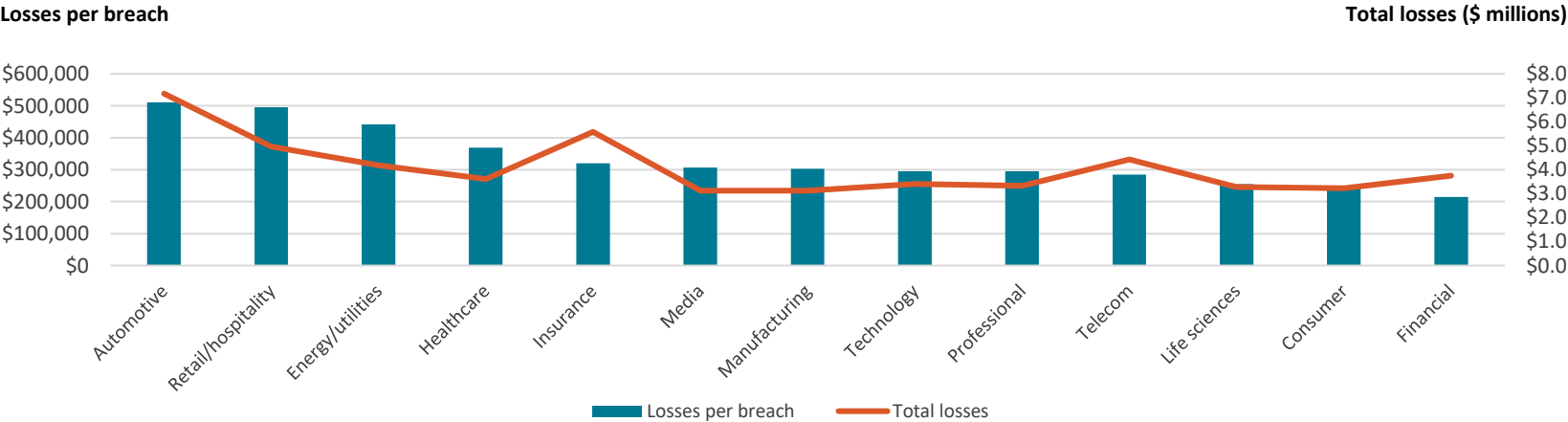
Q25: How many of the following categories of successful cybersecurity incidents did your company suffer last year and what is your estimate for this year?

The price tag per breach exceeds \$300,000

Over the most recent year, cyberattacks cost the 1,009 firms we surveyed \$4.1 billion, or an average of \$4.1 million per firm. This amounts to an average of about \$333,000 per breach.

This average represents the cost across all types of breaches—minor, moderate, and material. Using cost and breach data provided by each individual respondent, we calculated that the average cost per breach ranges from around \$215,000 for financial services firms—which reported the most minor and material breaches—to more than \$500,000 for automotive firms, which reported a significant number of material breaches. The size of the organization influences the size of the losses: for example, automakers are also among the largest companies, with an average revenue of \$27 billion. In contrast, the average revenue for consumer firms is less than half that at \$11 billion.

Cybersecurity losses per breach and total losses by industry (averages)



Q26: What were your total losses from cyberattacks last year and what is your estimate for this year?

The biggest companies suffer the largest cost per breach

The largest companies face the largest number of attempts—more than twice that of the smallest firms in our sample—as well as the steepest losses.

They also perform worse when it comes to managing the risks: one out every 2.7 attempts results in a successful breach for firms over \$20 billion, while for firms under \$1 billion, that number is 3.4.

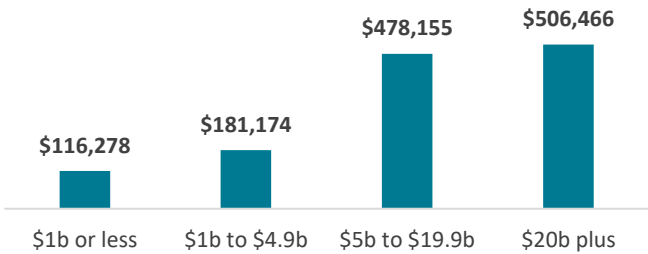
Larger firms suffer three times as many material breaches compared with the smallest firms. The biggest companies experience a greater number of moderate breaches, as well. Because of their greater proportion of moderate and material breaches, the largest enterprises are hit with a larger per breach cost than their smaller peers.

Big data breaches, which often attract substantial public attention, are particularly problematic for larger companies. They can not only face large financial losses and breach mitigation costs, but also fines and reputational impacts. This explains in part why cybersecurity is no longer just an issue at the company management level, but also at the board level. According to our survey, one-third of cybersecurity heads have greater interaction with the board and senior management, and 5% report to the board.

Attacks and breaches by firm revenue size

	Attempted attacks	Attempts per breach	Material breaches
\$1b or less	47	3.40	0.02
\$1b to \$4.9b	57	3.19	0.08
\$5b to \$19.9b	65	2.88	0.06
\$20b plus	108	2.72	0.06

Cybersecurity losses per breach by firm revenue size



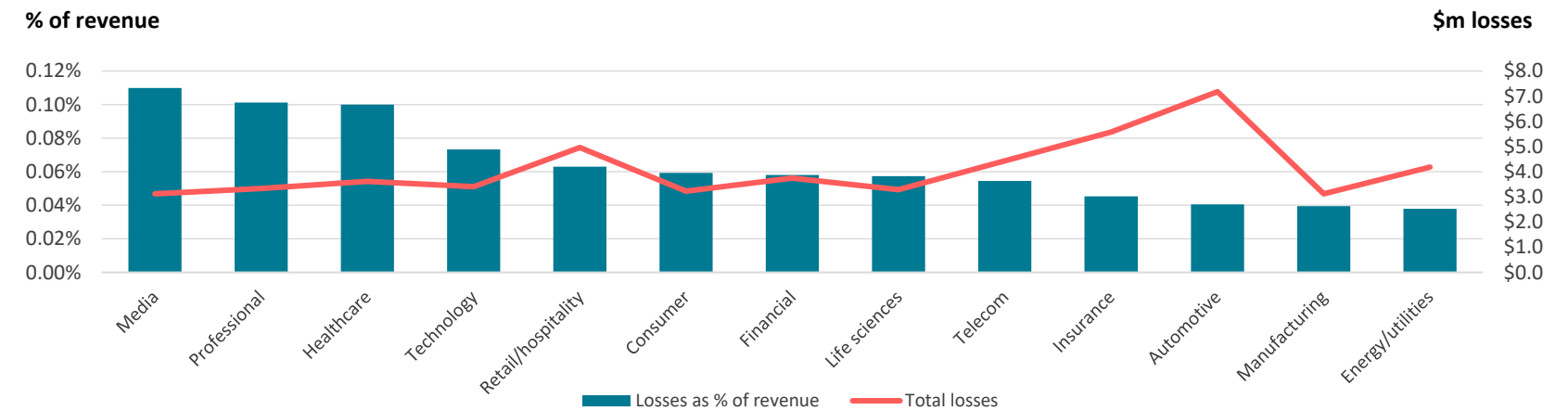
Q25: How many of the following categories of successful cybersecurity incidents did your company suffer last year and what is your estimate for this year?
 Q26: What were your total losses from cyberattacks last year and what is your estimate for this year?

Media, professional, and healthcare firms post highest losses

With billions of viewers, users, and fans connected through digital platforms, it is no surprise that media and entertainment companies are exposed and sustained the highest losses last year as a share of revenue, at 0.11%.

Although they suffered fewer breaches on average, cost per breach for media and entertainment firms was high, particularly because of their smaller size (an average revenue of \$5.3 billion, the lowest in our sample). The same pattern held for professional and healthcare organizations, with relatively high losses against lower average revenue. Automotive, manufacturing, and energy and utilities report the lowest losses, at 0.04% of revenue. At the time of the survey, firms were not expecting losses to change materially over the next year, but that may prove optimistic owing to the increase in risks during the pandemic.

Cybersecurity losses by industry (average)



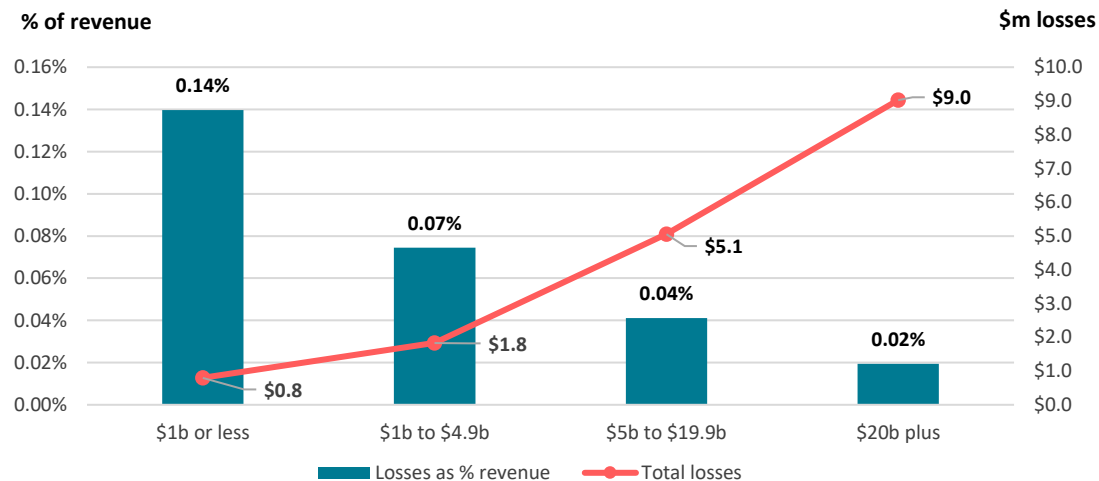
Q26: What were your total losses from cyberattacks last year and what is your estimate for this year?

Smaller firms face largest impacts from attacks

Companies with lower revenue experience the smallest losses in absolute terms, but the largest losses as a percentage of revenue.

Small firms see average losses of \$0.8 million, with a cost per breach of \$116,278, while large firms post average losses more than 10 times that size at \$8.9 million—a cost per breach averaging \$506,466, or five times as much. However, proportionately, small firms are much harder hit, with average losses seven times as large as a percentage of revenue as the losses of the largest firms (0.14% vs. 0.02%).

Cybersecurity losses by firm size



Q26: What were your total losses from cyberattacks last year and what is your estimate for this year?

“While all business types face the risk of cyberattacks, they are often most damaging to smaller companies that lack resources to sustain the costly expenses associated with a breach. As such, it is imperative that smaller businesses select the right technology to secure their borders.”

**Timothy Horton, VP,
Global Merchant
Security & Fraud, Fiserv**

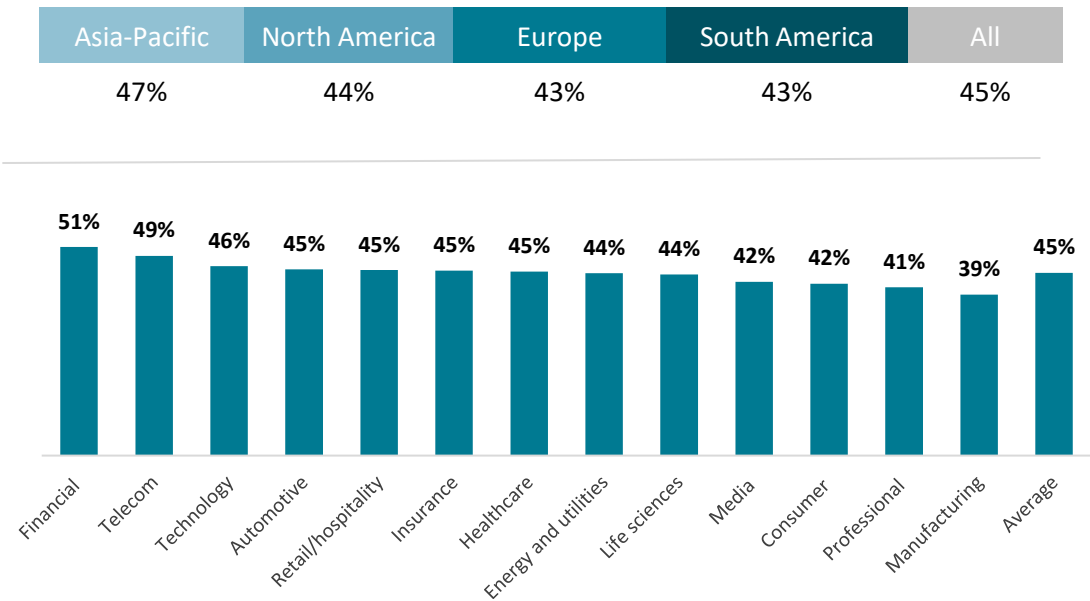
Average estimated probability of a successful breach is 45%

On average, firms estimate the likelihood of a successful breach over the next year at about 45%. However, this varies by industry and region.

Financial services firms and telecoms see the highest likelihood of a successful breach at around 50%; professional services and manufacturing, the lowest at about 40%. That is reasonably in line with their experience of breaches over the last year.

Asia-Pacific firms estimate a 47% likelihood of a breach vs. 44% for those in North America and 43% for firms in Europe and South America. In fact, APAC firms reported more than a third more total breaches than those in South America last year, so the larger estimate is reasonable. But this may be less the result of better security management in South America and more of better detection on the part of APAC companies.

Self-estimated probability of a successful breach



Q32: What is the likelihood (in percentage terms) that your business will experience at least one successful breach over the next year?

Firms underestimate the probability of a breach

Our analysis uncovered that most companies significantly underestimate the probability of a breach.

Based on the number of successful attacks that firms experienced over the most recent year, we have estimated probabilities for a moderate or material breach that are much higher than the self-estimated 45% average.

We calculate that insurance (86%), automotive (79%), and technology, financial, and telecom (all 77%) have the highest probability of a successful attack. Professional services (62%), media and entertainment (66%), and energy and utilities (67%) have the lowest probability.

The gap between self-estimated probabilities and our calculations are much greater in some industries, particularly insurance, manufacturing, and automotive. And since our estimates were based on the results of a pre-pandemic survey, they are likely to be conservative.

“CISOs often use qualitative metrics, such as high, low, to describe risk because most quantitative metrics don’t describe the actual level of risk and there isn’t sufficient data analytics to link these metrics to risk. Qualitative risk measurements describe whether the risk is bigger than a bread box.”

Jason Harrell, Executive Director, Technology Risk Management, DTCC

Industry	ESI-estimated probability	Self-estimated probability	Gap
Insurance	86%	45%	-41%
Automotive	79%	45%	-33%
Technology	77%	46%	-31%
Financial	77%	51%	-26%
Telecom	77%	49%	-28%
Manufacturing	75%	39%	-36%
Consumer	73%	42%	-31%
Retail/hospitality	72%	45%	-27%
Healthcare	72%	45%	-27%
Life sciences	70%	44%	-25%
Energy and utilities	67%	44%	-23%
Media	66%	42%	-24%
Professional services	62%	41%	-21%

Q32: What is the likelihood (in percentage terms) that your business will experience at least one successful breach over the next year?



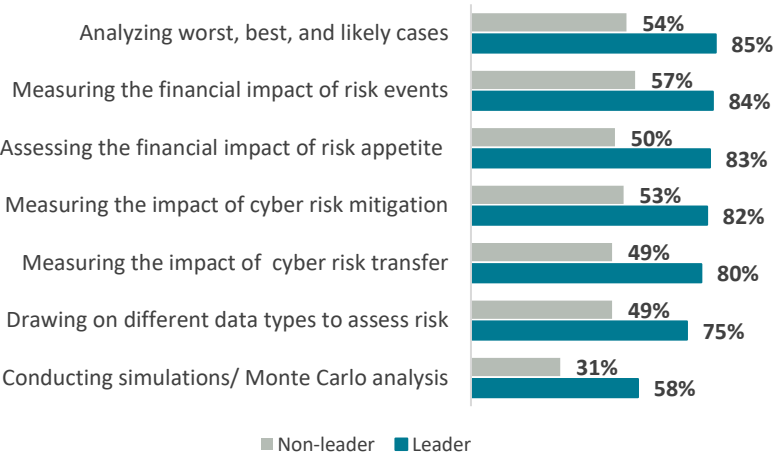
Mitigating and transferring risks

Understanding risk through quantitative analysis

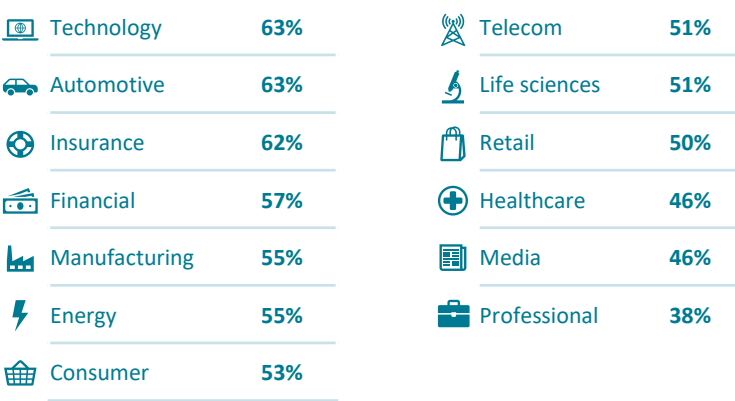
To properly understand their cybersecurity risk and how best to either mitigate or transfer it, companies—particularly leaders—are adopting a more analytically driven approach.

Eight in 10 leaders, and over half of all firms, use a bevy of analytical tools to measure risk and impacts. Technology, automotive, insurance, and financial firms are ahead in using quantitative methods to understand risk. One area that distinguishes leaders is scenario analysis, crucial for confronting black swan events. About 85% of leaders analyze worst, best, and likely cases, and 58% conduct simulations. According to Perry Carpenter, Chief Evangelist at KnowBe4: “It’s taking continuity and planning seriously, to the point where you’re doing essentially war games and tabletop exercises and analyzing third-party ripple effects.”

% of firms that are advanced/highly advanced



% advanced/highly advanced in all methods (averaged) by industry



Q11: What progress have you made in adopting a quantitative approach to risk management?

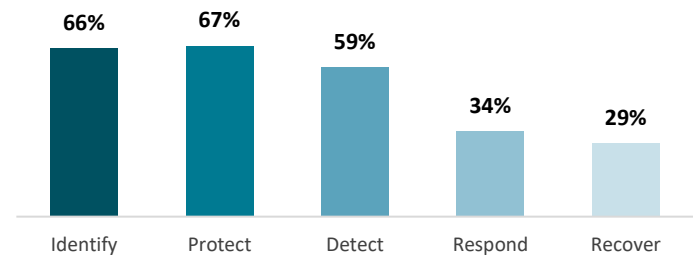
NIST compliance mitigates risk, but resilience needs more focus

Many firms use NIST compliance as a framework for risk mitigation and have made considerable progress on identification, protection, and detection. But they are behind on response and recovery, hindering their ability to cope with the pandemic.

Only about a third of companies have made notable progress on responding to breaches—and even fewer on recovering from them. While over half of cybersecurity leaders are advanced in resilience, they too have made less progress in these areas than in the other NIST pillars.

Firms with under \$1 billion in revenue are lagging more than others in response and recovery, with only about 1 out of 8 advanced in these pillars. This puts smaller companies under additional pressure when events like the pandemic occur.

Percentage of firms that made significant progress



NIST pillars	\$1b or less	\$1b to \$4.9b	\$5b to \$19.9b	\$20b plus
Identify	34%	58%	76%	92%
Protect	37%	57%	79%	92%
Detect	29%	50%	68%	86%
Respond	14%	19%	39%	65%
Recover	12%	21%	32%	52%

“Resilience has risen to the top of the agenda for the financial services sector. For CISOs, this requires thinking beyond protecting the network to forming integral partnerships across the organization that allow for a strategic approach to the rapid recovery of business operations in the event of an operational incident.”

Jason Harrell,
Executive Director,
Technology Risk
Management, DTCC

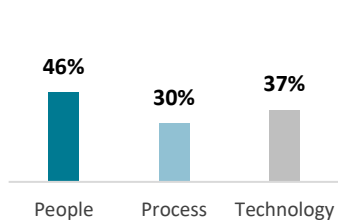
Q10: What progress have you made in each of the following cybersecurity functions, as prescribed, for example, by the US NIST’s cybersecurity framework?

Investing in people brings biggest reduction in risk

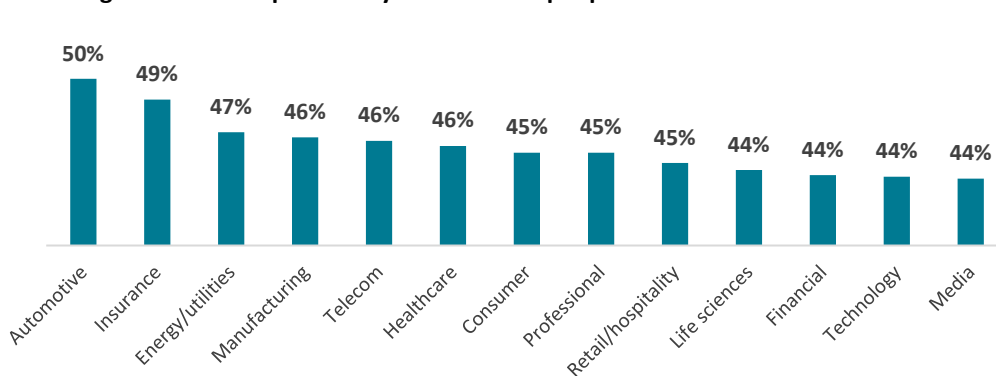
While people, process, and technology are all paramount for mitigating cybersecurity risks, firms report that investments in people reduce risk probabilities the most.

According to our research, on average, investments in people result in a 46% decline in the probability of a breach, more than investments in technology (37%) and process (30%). Automotive firms and insurers cite the greatest risk reductions from people investments. While technology can be easier for companies to implement, many CISOs believe the greatest value comes from developing a strong cybersecurity team and culture, with people trained to use that technology properly. “Ultimately, people are your biggest challenge, but also your biggest security advocates,” says Sean Ventura, CISO of Atmosera. “If you can get the culture of security embedded in everything that someone does, you’re going to increase your security posture significantly.”

Average reduction in probability of breach by investment area



Average reduction in probability of breach for people investments



“Only a small fraction of the CISO’s work involves bits and bytes. The important work involves influencing human behavior. This requires an understanding of psychology and economics as well as technology.”

Jon Nehlsen, Associate Dean, Heinz College of Information Systems & Public Policy, Carnegie Mellon University

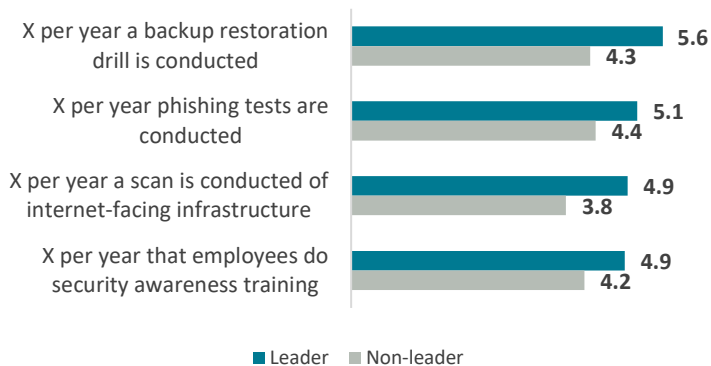
Q34: Please estimate the effectiveness of your investments in each of the following areas in reducing the probability of a breach.

Maintaining cyber hygiene is key for risk mitigation

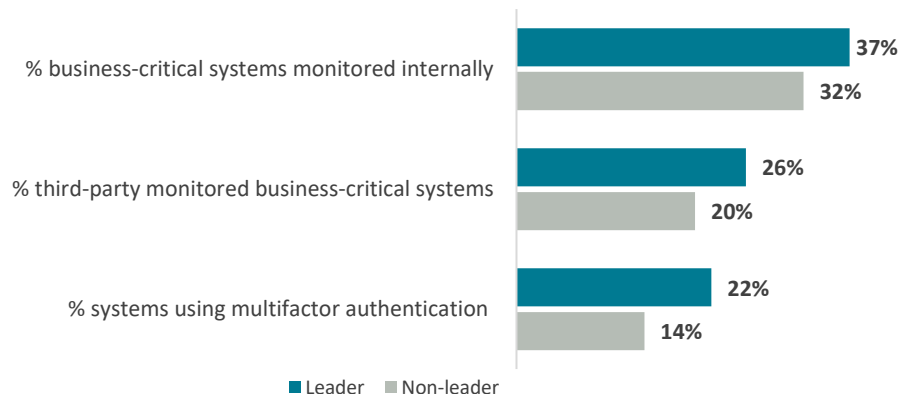
Keeping up with routine drills, scans, training, tests, and other hygiene practices is essential for reducing risk. Leaders do it better.

For cybersecurity experts, such as Ilan Abadi, Global CISO of Teva Pharmaceuticals, hygiene is a way of life—a lesson learned when he was CISO for the Israeli national police. So it is no wonder that cybersecurity leaders do more frequent backup restoration, phishing tests, security awareness training, maintenance of mobile devices, and installation of multi-factor authentication. Highlighting the importance of cyber hygiene, says one CISO: “You can’t spend your way out of cyber problems. It’s like exercising and eating right; you just have to wake up every morning and do it.”

Number of times per year firms test and train



% of systems maintaining best practices



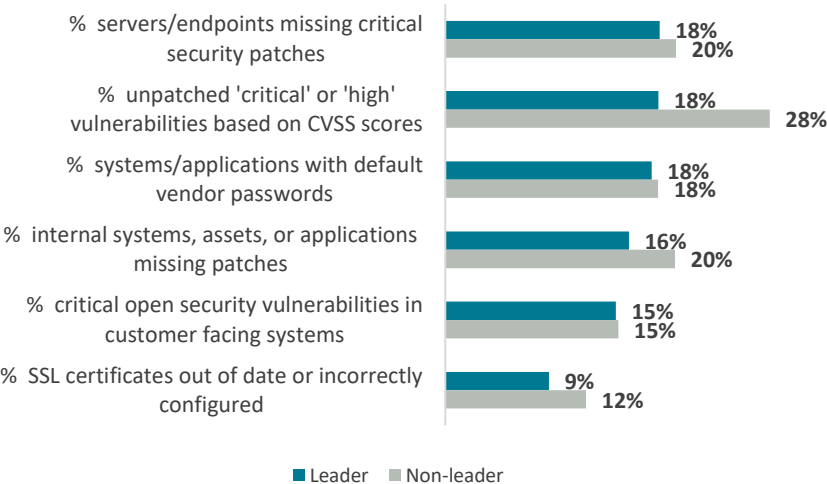
Q36: Please provide us with the latest data for the following cybersecurity metrics for the current year. Please fill in the average number of times per year or the percentage of systems.

Better cyber hygiene reduces risks for leaders

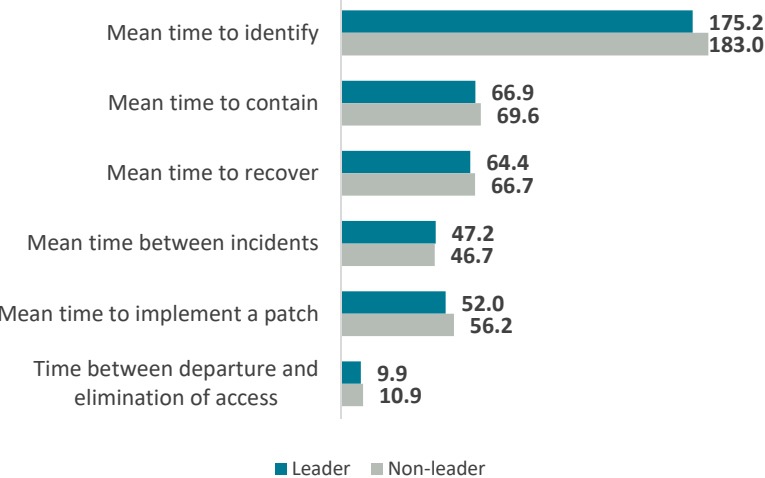
Leaders not only take more positive measures—they also avoid negatives by ensuring they complete basic tasks, thereby improving their performance.

Highly cyber-mature firms are particularly good at patching systems, whether they are servers and endpoints, critical vulnerabilities, or internal systems and applications. As a result, they do slightly better on some commonly used key performance indicators, and the days saved add up—ultimately reducing losses from risk incidents.

Average % of systems lacking necessary maintenance



Average number of days to complete task



Q35: Please provide us with the latest data for the following cybersecurity metrics for the current year. Please fill in the average number of days or the percentage of systems.

Transferring risk through cybersecurity insurance

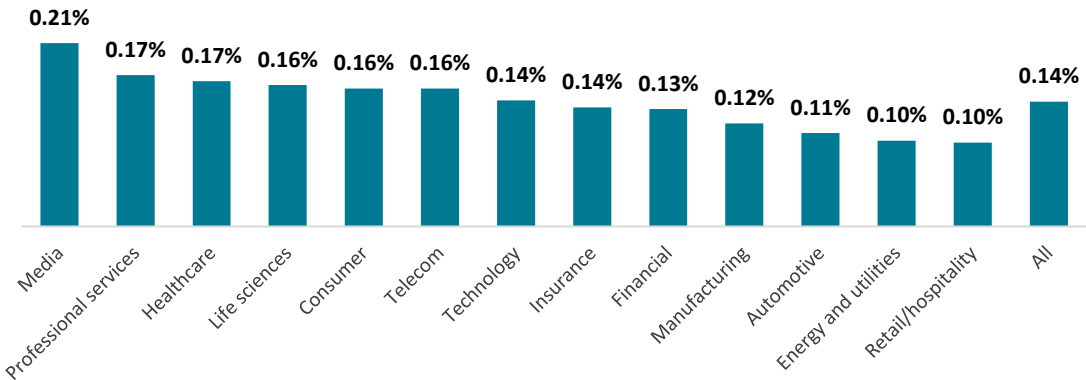
Firms must balance how much risk they want to manage and how much to transfer. On average, firms opt for cybersecurity insurance coverage of about 0.14% of revenue.

CISOs recognize that it’s impossible to address all risks—they could never spend enough time, money, and effort to do it. Nation-states can outspend them, and it just takes one hacker to get in. That’s where risk transference through insurance comes in. Our research shows a divergence of attitudes across industries: coverage limits range from 0.10% for retail/hospitality to 0.21% for media companies. While variations in coverage limits are reasonably in line with actual losses as a share of revenue for each industry, retail/hospitality firms appear to be underinsured, given that their losses are on the higher end. Coverage limits as a percentage of revenue tend to decrease as company size increases, because of economies of scale and of the smaller financial impact (as a share of revenue) on larger firms.

“You need to look at your risk appetite and at how much money you are going to spend to mitigate that risk. While cyber insurance does protect you in case of failure, it’s important to understand what you’re paying for, and the requirements of that insurance for due diligence and maintenance of best practices.”

Sean Ventura, CISO, Atmosera

Maximum cybersecurity insurance coverage as a % of company revenue



Q23: What is your company’s cybersecurity insurance coverage limit?

Companies plan to spend more on cybersecurity insurance

About 6 out of 10 firms plan to spend more on cybersecurity insurance over the next two years.

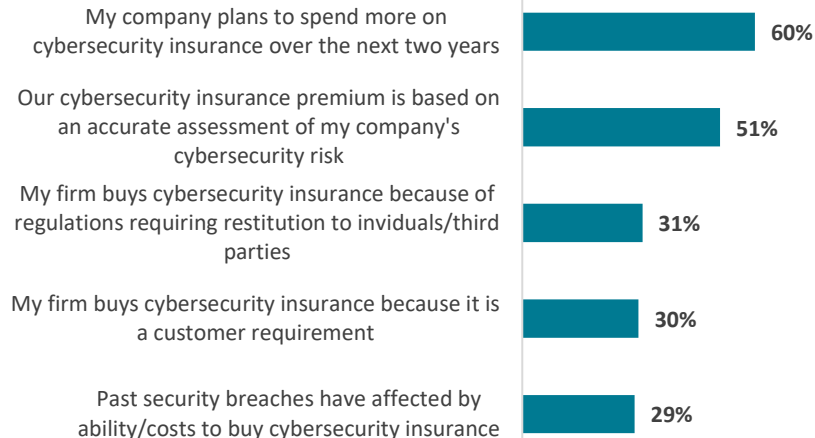
Companies buy cyber insurance for different reasons. The majority buy it for the protection it affords. In addition, about 3 out of 10 buy it because of regulations requiring restitution to third parties and a similar number buy it to comply with customer requirements.

Jack Kudale, CEO of Cowbell Cyber notes, “As organizations get comfortable with cyber insurance, and insurers offer tailored coverage that truly meets the needs of businesses, the concept of risk transfer through insurance will become mainstream.”

Cybersecurity leaders recognize that cyber insurance is a valuable tool that enables them to transfer the remaining risks that cannot be controlled by their cybersecurity systems. However, they also know that insurance should never be a substitute for putting the proper risk controls in place.



Corporate views on cybersecurity insurance (% agreeing)



57% of leaders have cyber insurance coverage over \$10m vs 30% of non-leaders

Q24: Do you agree or disagree with the following statements about cybersecurity risk insurance?

The role of insurance in cybersecurity programs



“Firms must balance their cyber risk management programs between the risks they decide to manage internally and the point where it is more cost effective to transfer the risk, such as insurance. It is also important when making decisions on insurance that firms understand the risks they want to transfer and the coverage they have through other corporate insurance vehicles.”

Jason Harrell, Executive Director, Technology Risk Management, DTCC



“We use cyber insurance, but it doesn’t alleviate my responsibility for managing or reducing a risk, it’s simply a financial offset. We still have an incident response plan. We still have incident handlers. We still have subject matter experts who we can call to help us if we need them. Hopefully, I never have to call our insurance firm. If I do, that means we’re busy trying to put out a wildfire of some sort and there’s been a major disruption.”

Jeffrey Coe, CISO, ON Semiconductor



“Cyber insurance is a key aspect of any cybersecurity program. The chances are that most of the projects or products that your company is rolling out will have some risk. It’s not worthwhile to close all those risks.”

“When thinking about insurance, CISOs need to consider the difference between controlled and uncontrolled risks. Insurance is valuable for addressing the unknown unknowns.”

Chintan Jain, Founder & VP of Security Engineering, Security Mantra



Case Study

Taking a holistic approach to mitigating risk



Ron Mehring,
VP Technology &
Security, Texas
Health Resources

Texas Health Resources has changed the way it looks at risk from a piecemeal approach to one that is more holistic and rigorous, and includes risk modeling, risk registers, and a detailed risk narrative for each set of systems and controls. It then does a risk tolerance mapping and a determination of investments needed to drive the risk down to acceptable levels.

“There will be different opinions about how much risk we should take from different groups,” says Ron Mehring, VP Technology & Security. “Where you put that tolerance level is where your cost is. If you want to reduce risk by 50%, that’s a cost; if you want to reduce it by 100%, that’s an enormous cost. The toughest risks to remediate are the last 5%—which could be the difference between spending \$10 million on a security program or \$100 million.”

Insurance is one solution, according to Mehring. “If we’re going to get a large risk-transfer cyber insurance policy that we pay a premium for every year, we need to understand the relationship between that premium and that risk transfer, and compare that risk financing against potential losses,” says Mehring.

He explains that Texas Health must consider the impact of losing all 10 million patient identities, or whether it should assume that it might lose 80,000-150,000 identities per year and plan its insurance around that level of loss. “We definitely aren’t designing for the black swan event because that’s hard to do. That may be where insurance can help, but you need to weigh the costs.”

“The CISO is really becoming a risk manager. Sure, we must understand the technical underpinnings and how things work. But many of us are transitioning from a very technology-centered position to somebody who’s interacting with enterprise risk programs and articulating what these types of major decisions mean to a company.”



The ROI of cybersecurity

Calculating the ROI of cybersecurity investments

The ROI of cybersecurity is more complex than the ROI of most other investment decisions that a firm might make, since it is based on a reduction in losses rather than an increase in returns.

We focused our ROI analysis on how cybersecurity investments change a firm's expected losses (EL), building on the work of Douglas Hubbard and taking a Bayesian approach to assessing cybersecurity risk. To calculate the baseline EL before the investment, we used Monte Carlo analysis with the respondents' own estimates for the probability that they will suffer a successful breach over the next year, combined with their own lower and upper bound estimates for the potential loss from such a breach. We chose to use respondent's self-estimated probabilities rather than our own, higher estimates because those generated more conservative ROI results.

We then adjusted the probability of a loss based on the firm's estimate for effectiveness of their investments in people, process, and technology in reducing the probability of a breach. We calculated the expected loss using the new probabilities. The difference between the baseline expected loss and the adjusted expected loss represents the benefits of that investment. We compared those benefits against the investment to calculate the ROI. We did 10,000 iterations of this Monte Carlo analysis individually for each respondent firm, averaging the results to arrive at the estimated ROI for each firm. We then averaged ROI estimates across maturity levels and industries.

The Hubbard formula for calculating cybersecurity ROI



$$\text{Cybersecurity ROI} = \frac{(\text{EL before the investment} - \text{EL after the investment} - \text{cost of the investment})}{\text{cost of the investment}}$$

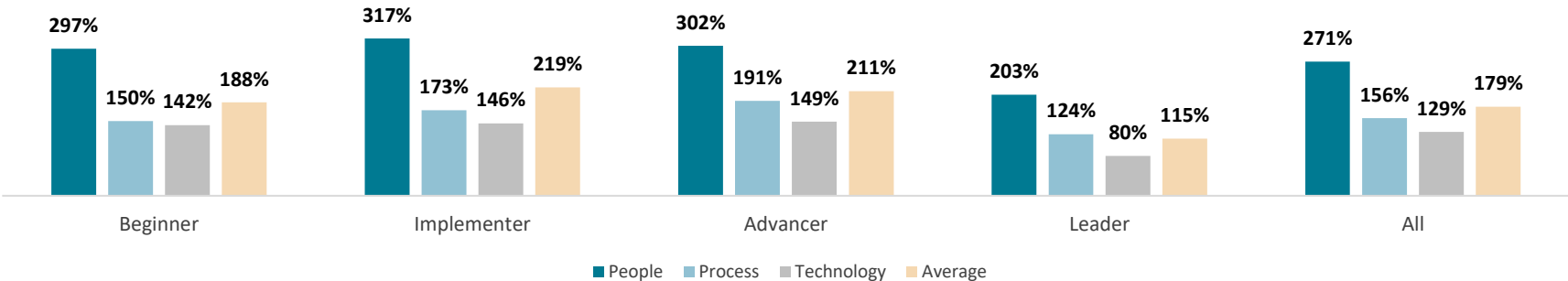
Cyber investments can generate enormous ROI

On average, organizations see an overall ROI of 179% from their cybersecurity investments. That means that every dollar invested generates close to \$2 in benefits.

The ROI ranges from 271% for investments in people, 156% for process, and 129% for technology. These figures would be even larger using ESI ThoughtLab’s higher estimates for probability of a breach. However, not all firms surveyed generate a positive ROI for their cybersecurity investments—about a third have estimated negative returns.

Firms in early stages of cybersecurity maturity (beginners and implementers) can recognize very high ROI, since they take basic steps that can have outsized benefits. But there are diminishing returns as firms become more mature and tackle more challenging risks. Enterprises already at the highest level of maturity will need to be more circumspect to ensure an adequate return on their next level of cybersecurity investments.

ROI by investment area and maturity

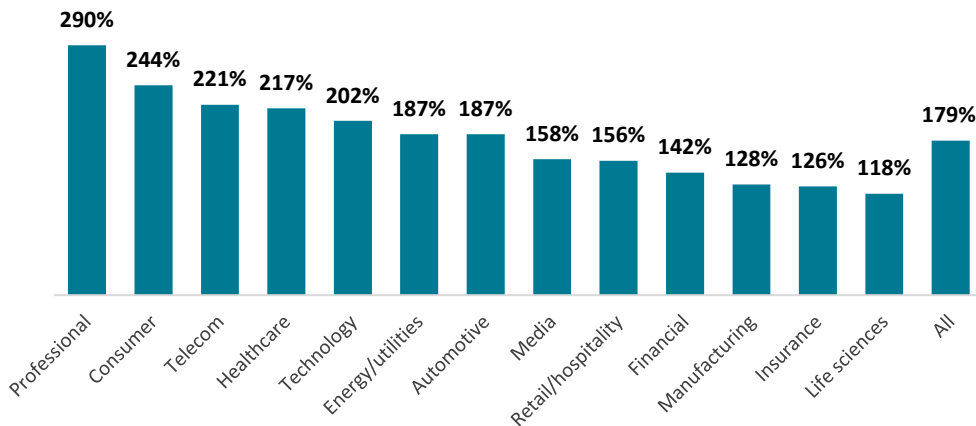


ROI varies by size and industry

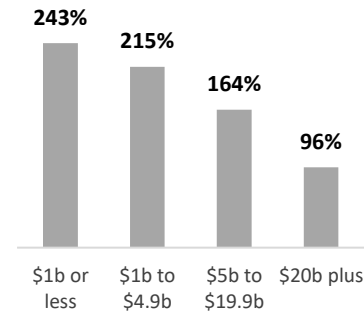
As firm size increases, ROI diminishes. That is partly because larger companies tend to be more advanced in cybersecurity. They are also more complex and expensive to protect.

The industries with the highest overall ROI are professional services, consumer products, and telecom. Those with the lowest are manufacturing, insurance, and life sciences—but all nonetheless see substantial returns. Across industries and maturity levels, firms get the largest ROI from their investments in people, followed by process, then technology. However, regardless of industry or maturity, firms are spending the largest portion of their budgets on technology.

ROI % by industry



ROI % by company size



“Calculating ROI is data-driven. The efficiency of an organization, the number of vulnerabilities, and spending are measurable across industries. I can show ROI in terms of efficiency and times savings, or cost savings or avoidance. There are numbers around how much a data breach costs.”

Sean Ventura,
CISO, Atmosera

The benefits of cybersecurity investment go beyond ROI

The top benefits from cybersecurity are enabling digital transformation and building trust with customers.

Companies constructing a business case for investing in cybersecurity should consider the upside of these investments. In addition to trust and transformation, benefits include growing shareholder value, enabling innovation, building market share, and driving revenue growth. Cybersecurity leaders show the way, teaming up with heads of internal business units to facilitate their growth strategies and operational plans.

% recognizing as business benefit from improved cybersecurity

	Leader	Non-leader	All
Enabling progress on digital transformation	69%	62%	64%
Building customer trust	68%	67%	68%
Growing shareholder value	52%	31%	36%
Enabling innovation and speed to market	47%	37%	40%
Building competitive advantage and market share	40%	33%	36%
Driving revenue growth and sales	38%	30%	32%
Reinforcing reputation for high standards and CSR	37%	36%	37%
Attracting, retaining, and developing business with customers	32%	40%	40%
Improving government relations and overseas opportunities	31%	25%	27%
Improving product quality and demand	28%	31%	33%

“If the CMO’s job is to get the company in the news, the CISO’s job is to keep the company out of the news! By establishing a culture of understanding specific to cybersecurity, the CISO should endeavor to turn the entire organization from a potential liability to an asset.”

**Edwin Doyle, Global Security Strategist,
Check Point Software**



Q31: What business benefits, if any, has your company recognized through improved cybersecurity?

Case Study

Partnering with the business to build ROI



**Jeffrey Coe, CISO,
ON Semiconductor**

For Jeffrey Coe, CISO at ON Semiconductor, demonstrating return on investment for cybersecurity revolves around the company's objectives. His group's approach to cybersecurity is as a partnership with the business, dedicated to helping it to achieve its goals.

"Our mission is to be one of the premier semiconductor manufacturers on the planet, not the most advanced cybersecurity company on the planet that happens to manufacture semiconductors," he says. "We are here to support the strategies of the business. If difficult business decisions or opportunities drive risk a bit higher than any of us are comfortable with, that's okay. Measured risk is what we should be taking."

Coe works closely with executives in different parts of the company and while he cannot, as they do, show a revenue stream resulting from investments in cybersecurity, he focuses on risk reduction. "I live and breathe that risk model because that's how we've been successful at gaining attention and sponsorship. Our approach is, if the company wants to do a certain activity, or penetrate a particular market, here is what we need to have in place to achieve that level of revenue or win that business."

He says that cybersecurity excellence is about helping the company build competitive advantage, grow market share, and win with customers. "My job is to keep our company's secrets secret, and to help different parts of the business do what's important to them without disruption. Security for the sake of technology is not our mission—we're trying to help our colleagues win."

The COVID-19 pandemic has only highlighted this focus for Coe. "This is a matter of what our company needs to do to remain competitive and viable. It's about how we win that next deal, squeeze out products more efficiently, or bring on a new supplier, because we have to generate revenue or reduce costs, otherwise outcomes could change for us."

In this environment, the CISO must help management make risk-based decisions without becoming a hinderance to the company's profitability. "It's been an epiphany for us," he says. "The pandemic and the mobile workforce have brought to the forefront things we knew to be true, but now we are seeing them play out in real time."



Calls to action

Calls to action



1. Take a proactive approach. “The biggest cybersecurity issue most organizations face is not a technology issue, but rather one of mindset. Many organizations simply don’t know where to start or what to tackle next. Such organizations easily get caught in a cycle of reaction: simply being led around by the latest threat-of-the-day, tech-of-the-day, or breach-of-the-day. That approach leads to confusion, inefficiency, or apathy.”

Perry Carpenter, Chief Evangelist, KnowBe4



2. Don’t make cybersecurity an afterthought. “As an insurance company, we’re in the risk management business. With every single decision we make, we must ask ourselves how much cybersecurity risk do we want to assume and what steps should we take to mitigate it? The most important thing as you’re doing your digital transformation is embedding cybersecurity from the start, not coming back from the end. It sounds really simple, but rarely does it happen in most companies.”

Nimesh Mehta, SVP and CIO, National Life



3. Layer your defenses. “Our approach is a defense-in-depth strategy. It’s not necessarily just about perimeter defenses, as it was in the past. It’s now all about understanding your controls, understanding your access, and segmenting and encrypting data in a layered fashion so that you can protect people throughout the organization.”

John Marcante, CIO, Vanguard



4. Keep your tool stack short and tailored to your needs. “We have just five primary tools, but they’re being used to the maximum potential. That’s allowed our team to really learn, develop, and extract the most value out of these tools, rather than embracing the latest and greatest tool that comes out from a security vendor. We have a good understanding of the risks within our business. Our tooling is built to directly address those risks.”

Juan Morales, Deputy CISO, Realogy

Calls to action



5. Avoid knee-jerk reactions. “It’s better to first really understand your organization and how a response may apply to your own particular situation. Then make an informed decision on what should be done next.”

Jason Harrell, Executive Director, Technology Risk Management, DTCC



6. Be agile and able to adapt. “How quickly can I move? How quickly can I accept failure and move on? How quickly can I say, I need to think out of the box and here are my constraints? You need to adjust on the fly, and there are no books, articles, or things written around that. Understand that you can fail and still be successful at the same time.”

Richard Rushing, CISO, Motorola Mobility



7. Double down on identity and access management. “In most organizations, that’s the top priority in the budget, and it should be. If you focus on doing those two things well with robust multi-factor authentication and asset management with good vulnerability management, you’re going to be in a decent place.”

Joe Sullivan, CSO, Cloudflare



8. Find the right balance. “To be successful, companies need to balance the fundamentals of people, process, and technology. Firms are hiring the best talent they can afford, building consistency in operations through automation and well-vetted cyber risk assessments, and tracking threats and innovating with responsive AI technologies. As part of these investments, CSOs need to mitigate new risk and the potential for cyber crime by evaluating preventative practices and cyber insurance policies for protection.”

Mike Convertino, CSO, Arceo.ai

Calls to action



9. Understand you can't do it all on your own. "You can't control all of the risks that are out there or deal with everything with the same attention. In some cases, you need to do a risk transfer, like cyber insurance. Also, today there are lots of services that can help with risk assessment, for example vendor risk. You don't have one answer or approach to deal with everything yourself. It's an ecosystem of risk that you have to manage."

Ilan Abadi, Global CISO, Teva Pharmaceuticals



10. Be mindful of IoT, which represents the next generation of cyber threats. "IoT devices have found their way into all aspects of our lives. Devices such as smart TVs, IP cameras, manufacturing sensors, and medical devices are now commonplace in many organizations. However, connecting them to your network is triggering a new category of dangerous cyber threats."

Chris Scanlan, President of Americas, Check Point Software



11. Keep your eye on the ball. "While companies may see their revenue shrink in the wake of the pandemic, they should not let that deter them from spending what they need on security. They should bear in mind how much their most important assets cost them and the probability that someone will try to steal them, whether it's customer records or trade secrets. Even in times of uncertainty, threat actors are not going to go away, the regulations remain, and fines are not going to decrease."

Chintan Jain, Founder & VP of Security Engineering, Security Mantra



12. Understand that compliance does not equal security. "Compliance is like a snapshot-in-time that validates what you believe to be true, based on the evidence you have gathered. Security, on the other hand, is like a video of what is happening, using regular metrics, monitoring, and adjusting based on business goals. To build a world-class security program, you need to maintain your cybersecurity technology investments and move them toward where your business stakeholders want to go."

Jeffrey Coe, CISO, ON Semiconductor

Calls to action



13. Boost your cyber risk assessment capabilities.

“The focus in the industry is shifting from prevention and detection to cyber risk assessment. In the next 3-5 years, the process of quantifying cyber risks in terms of financial impact will become systematically integrated with the pursuit of digital initiatives.”

Jack Kudale, Founder and CEO, Cowbell Cyber



14. Accept that breaches are a reality. “One game changer has been the gradual shift in attitude toward cyber incidents. No longer are they automatically career-ending events with the CISO taking the blame. Accepting that bad cyber events can occur has freed security personnel to align their activities to the risk appetite of the company.”

Brian Wrozek, VP, Corporate Security, Risk and Compliance Management and Physical Security, Optiv



15. Strengthen your defenses where it matters.

“Simple financial gain is often the major incentive driving cyber criminals to exploit system vulnerabilities or human error. There is a lot that organizations can now do to protect themselves, including tracking common patterns within cyberattack journeys and using this information to strategically enhance security defenses in the places that matter the most. This can be a game changer in fighting cybercrime.”

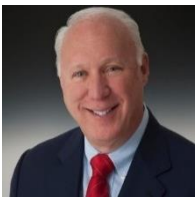
John Loveland, Global Head of Cybersecurity Strategy & Marketing, Verizon Business



16. Communicate well and regularly. “Consumers increasingly expect organizations to be accountable for the data they collect, share, and use. Organizations will be challenged to ensure their data privacy policies align with the regulatory demands under GDPR and the CCPA, while also meeting stakeholder expectations for clear and transparent communications. How companies approach communications readiness for cyber risks in the COVID-19 environment also will need to evolve.”

Jamie Singer, Senior VP, Crisis & Risk Management, Edelman

Calls to action



17. Cyberattacks can be sophisticated: you need to be too. “Attackers are constantly upping their game, so we need to improve ours. We have moved beyond thinking of cybersecurity as simple adherence to an operational checklist. Cyber threats and defenses must be integrated into core business functions and assessed in terms of their economic value to the enterprise. Cyber investments often have positive ROI, but not always. A sophisticated defense includes proactive analysis of likely threats and calibrated defenses to assure ROI and security.”

Larry Clinton, President, Internet Security Alliance



18. The time to act is now. “COVID-19 is accelerating digital adoption globally, transforming everything from how we pay for goods to how employees show up to work every day. Businesses that take the appropriate measures now to secure their digital borders—and data and information held within—will benefit as digital interactions dominate.”

Timothy Horton, VP, Global Merchant Security & Fraud, Fiserv



Sponsors and advisors

Our sponsors and advisors

Driving Cybersecurity Performance: Improving results through evidence-based analysis was sponsored by a diverse coalition of companies that specialize in cybersecurity technology solutions and insurance.

Each organization is an expert in its domain and would be happy to share its insights on the research results and what they mean for your business. They can help you benchmark your company's approach with your peers in the study through use of our benchmarking platform and database.

We were also fortunate to have a group of distinguished research advisors and media partners that provided valuable inputs and guidance throughout the project.

We would like to thank our sponsors, research advisors and media partners for helping us develop this ground-breaking study.

Lead sponsors



Supporting sponsors



Media partners



Research Advisors



Advisory board

Sponsors

Name	Title	Company
Davis Hake	Business Development and Co-Founder	Arceo.ai
Dan Prince	Communications Lead	Arceo.ai
Cindy Wilson	Head of Corporate Marketing	Check Point Software
Lloyd Tanaka	Manager, Content Marketing	Check Point Software
Isabelle Dumont	VP, Market Engagement	Cowbell Cyber
Timothy Horton	VP, Global Merchant Security & Fraud	Fiserv
Perry Carpenter	Chief Evangelist and Strategy Officer	KnowBe4
Kathy Wattman	Senior VP, Public Relations	KnowBe4
J.D. Padgett	Senior Market Research Analyst	Optiv
John Loveland	Global Head, Cybersecurity Strategy & Marketing	Verizon Business

Advisors

Name	Title	Company
Timothy McNulty	Associate VP, Government Relations	Carnegie Mellon University
Jon Nehlsen	Associate Dean, Heinz College of Information Systems & Public Policy	Carnegie Mellon University
Jason Harrell	Executive Director, Technology Risk Management	DTCC
Larry Clinton	President	Internet Security Alliance
Peter Keenan	CISO	Lazard
Chintan Jain	Founder & VP of Security Engineering	Security Mantra Corporation
Ambareen Siraj	Founder & Board Member	Women in Cybersecurity

Media Partners

Name	Title	Company
Patrick Hillman	Executive VP, Crisis & Risk Management	Edelman
Jamie Singer	Senior VP, Crisis & Risk Management	Edelman
Rob Sloan	Cybersecurity Research Director	WSJ Pro Cybersecurity
Will Wilkinson	General Manager	WSJ Pro Cybersecurity

Executive interviews

Name	Title	Company
Perry Carpenter	Chief Evangelist & Strategy Officer	KnowBe4
Brian Jack	CISO	KnowBe4
Jason Harrell	Executive Director, Technology Risk Management	DTCC
Peter Keenan	CISO	Lazard
Ronald Mehring	CISO	Texas Health
Chintan Jain	Founder & VP of Security Engineering	Security Mantra Corporation
Joe Sullivan	CISO	Cloudflare
Sean Ventura	CISO	Atmosera
Richard Rushing	CISO	Motorola Mobility
Edwin Doyle	Global Security Strategist	Check Point Software

Name	Title	Company
Chris Scanlan	President of Americas	Check Point Software
Jamie Singer	Sr Vice President, Crisis & Risk Management	Edelman
Davis Hake	Co-Founder	Arceo.ai
Mike Convertino	CSO	Arceo.ai
Juan Morales	Deputy CISO	Realogy
Brian Wrozek	VP, Corporate Security, Risk & Compliance Management & Physical Security	Optiv
Ilan Abadi	Global CISO	Teva Pharmaceuticals
Jeffrey Coe	Senior Director and CISO	ON Semiconductor
John Marcante	CIO	Vanguard
Nimesh Mehta	CIO	National Life



ESI THOUGHTLAB

Driving Cybersecurity Performance: *Improving results through evidence-based analysis*
has been produced by ESI ThoughtLab, a leader in thought leadership initiatives.
To learn more about ESI ThoughtLab, visit: www.esithoughtlab.com.

