

The Cybersecurity Imperative

Managing cyber risks in
a world of rapid digital change

An interactive thought leadership report

Produced by

ESITHOUGHTLAB

In conjunction with

WSJ PRO CYBERSECURITY



Sponsored by: **Baker McKenzie.**

 CyberCube



KnowBe4
Human error. Conquered.

 opus

protiviti®
Face the Future with Confidence

SIA
SECURITY INDUSTRY ASSOCIATION


Willis
Towers
Watson



Introduction

By 2021, cybercrime is likely to cost the world \$6 trillion annually*, more than the combined GDP of the UK and France. As firms embrace latest technologies and respond to rising regulations, cybersecurity has become a top management priority across industries and markets.

Cybersecurity is a moving target: as companies adopt new technologies, so do hackers. The reluctance of firms to share cybersecurity information makes benchmarking and planning more challenging. To fill this gap, ESI ThoughtLab joined with WSJ Pro Cybersecurity and a group of leading organizations to launch *The Cybersecurity Imperative*, a thought leadership program drawing on rigorous global research and analysis.

This interactive report presents insights into cybersecurity best practices, performance metrics, and calls to action. We hope it helps you meet the challenges of today's complex and an ever-changing cyber risk landscape.



Louis Celi
Chief Executive Officer
ESI ThoughtLab



Daniel Miles, Ph.D.
Chief Economist
ESI ThoughtLab

How we did the research

We conducted four types of research:

1. A diagnostic survey of 1,300 firms across industries and regions.
2. In-depth interviews with 18 CISOs and cybersecurity experts.
3. Insights from an advisory board of executives with a variety of views.
4. Modeling the impact of cybersecurity practices on performance.

Our benchmarking model segmented companies into three stages of cybersecurity maturity: **beginners, intermediates** and **leaders** by scoring their reported progress in each activity of the NIST cybersecurity framework's five categories, using a 0-4 ranking. We summed the activity scores to arrive at a company's composite score for each category and overall.

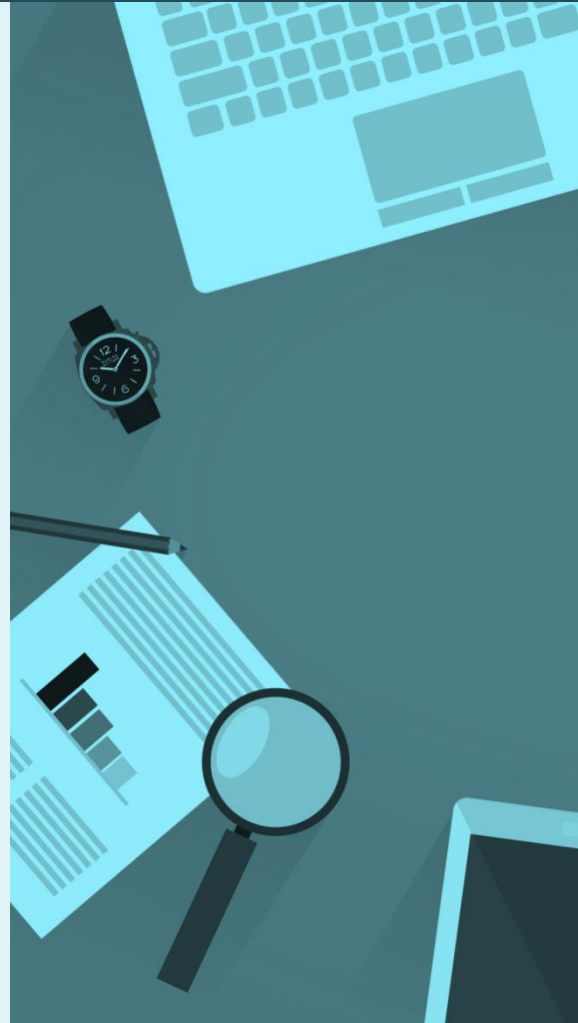
*According to [Cybersecurity Ventures](#)

[Introduction](#)
[Executive Summary](#)
[Evolving Risk Landscape](#)
[Road to Excellence](#)
[Organizing for Cybersecurity](#)
[Managing Cyber Risks](#)
[Economics of Cybersecurity](#)
[Measuring Cyber Risks](#)
[Calls to Action](#)
[Research Background](#)
[Acknowledgements](#)

Executive Summary

“We are facing an urgent crisis in cyberspace. The CAT 5 hurricane has been forecast, and we must prepare.”

Kirstjen Nielsen, US Homeland Security Secretary

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Executive summary

- 1. The speed of digital transformation is heightening cyber-risks for companies as they embrace new technologies, adopt open platforms, and tap ecosystems of partners and suppliers.** While firms now report the biggest impacts from malware (81%), phishing (64%), and ransomware (63%), in two years, they expect massive growth in attacks through partners, customers, and vendors (+247%), supply chains (+146%), denial of service (+144%), apps (+85%) and embedded systems (84%).
- 2. Cybersecurity is further complicated by the “digital backlash.”** When digital transformation outpaces cybersecurity progress, companies bear a bigger chance of suffering a major cyber-attack (over \$1m in losses). Digital leaders in early stages of cybersecurity have 27% chance of suffering a major attack, compared with a 17% probability for digital leaders with advanced cybersecurity systems.
- 3. While companies see high risks from external threat actors, such as unsophisticated hackers (59%), cyber criminals (57%), and social engineers (44%), the greatest danger, cited by 9 out of 10 firms, lies with untrained general (non-IT) staff.** In addition, more than half see data sharing with partners and vendors as their main IT vulnerability. Nonetheless, less than a fifth of firms have made significant progress in training staff and partners on cybersecurity awareness.
- 4. To cope with rising risks, companies upped their cybersecurity investment by 7% over the last year and plan a 13% boost next year.** The biggest upsurge is coming from platform companies, which hiked their investment by 58% over the last year, and plan an even larger bump next year. Energy/utility firms are planning to increase spending 20%, technology (15%), consumer markets (14%), insurance (13%) financial services (12%), and life sciences/healthcare (10%). The only standout is manufacturing, which is planning to raise spending by only about 1%.
- 5. Cybersecurity investments will vary by company size and location.** Companies under \$5 billion will raise spending at almost triple the average of 13%. Firms with revenue between \$250m-\$1b will spend \$2.8m next year, \$1b- \$5b (\$5.2m), \$5b-\$20b (\$9.6m), and \$20b+ (\$14.5m). Firms with less than \$1 billion in revenue are increasing their spending by 33% and those with \$1-5 billion by 30%. Companies based in South Korea, which face higher risks from government sponsored attacks, will increase their investment by more than double the average, as will those in Mexico and Australia. Firms in China, Singapore, Argentina, the US, and Canada will also boost spending at a higher than average rate.

Executive summary

- 6. Next year, companies will allocate 39% of their cybersecurity budget to technology, 31% to process, and 30% to people.** Firms now use a variety of technologies, from multi-factor authentication (90%) and blockchain (68%) to IoT (62%) and AI (44%). Over the next two years, there will be an explosion in the use of technologies such as behavioral analytics (which will increase by over a factor of 18), smart grid technologies (nine-fold), deception technology (seven-fold), and hardware security and resilience (more than double).
- 7. Companies with the highest cybersecurity maturity scores (over the average of 100) are the US (107.2), South Korea (104.7), Japan (102.6), France (101.9), Australia (101.3), and Spain (101.1).** Most of the lowest scoring companies are based in emerging markets, including Mexico, India, Argentina, and Brazil, although firms in Germany and Switzerland also had relatively low scores.
- 8. Companies are now investing more in cyber-risk prevention/detection than in resilience.** While companies will increase their investment in protection next year to 26%, they will also allocate more to respond (19%) and recover (18%) and less than they did this year to identify (18%) and detect (18%).
- 9. As cybersecurity systems mature, the probability of costly cyberattacks declines.** Cybersecurity beginners have a 21.1% probability of a cyberattack generating over \$1m in losses vs. 16.1% for intermediates and 15.6% for leaders. The costs of cyberattacks also fall sharply with maturity: for a company with \$10 billion in revenue, costs would average \$3.9 million if the company were a beginner, while if it were a leader, they would average \$1.2 million. And beginners may be underestimating costs due to ineffective detection systems.
- 10. Companies are reorganizing to improve cybersecurity:** Cybersecurity leaders (37%) are more likely to assign responsibility to a CISO than beginners (20%). For beginners and companies with under \$1 billion in revenue, the board is more likely to have primary responsibility. However, worldwide regulatory changes are making a chief privacy or data protection officer role more common and sometimes integrated with the role of the CISO, particularly in companies with over \$20 billion in revenue.

Executive summary

- 11. As firms move up the cybersecurity maturity curve, the ratio of cybersecurity to technology staff drops.** One reason is that the need for specialists falls as firms install automated cybersecurity systems and tap advanced technology, such as robotics and AI. Another is that leaders make better use of cybersecurity ecosystems, relying more on partners and suppliers and increasingly outsourcing their cybersecurity work.
- 12. Calculating the ROI of cybersecurity is elusive for most firms.** One stumbling block is that companies often do not measure indirect costs, such as productivity loss, reputational damage, and opportunity costs, which can seriously hurt bottom lines. Another is the difficulty of gauging risk probabilities and costs avoided from tighter cybersecurity. Finally, companies measure risks, and not the upside from improving productivity, profitability, corporate reputation, competitive positioning, and customer engagement—which were cited as cybersecurity benefits.

Key takeaway

To avoid the digital backlash, integrate cybersecurity into every stage of digital transformation and measure the return on investment on an ongoing basis. Companies should focus on cybersecurity at the start of the digital transformation process, not at the end. Rather than a silo approach, cybersecurity should be embedded within the business teams that are driving innovation. At the same time, companies should do more to measure the ROI on their cybersecurity initiatives, taking into account both the direct and indirect costs and the upside from securing their digital futures.

Evolving Risk Landscape

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

Kevin Mitnick, Chief Hacking Officer, KnowBe4

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

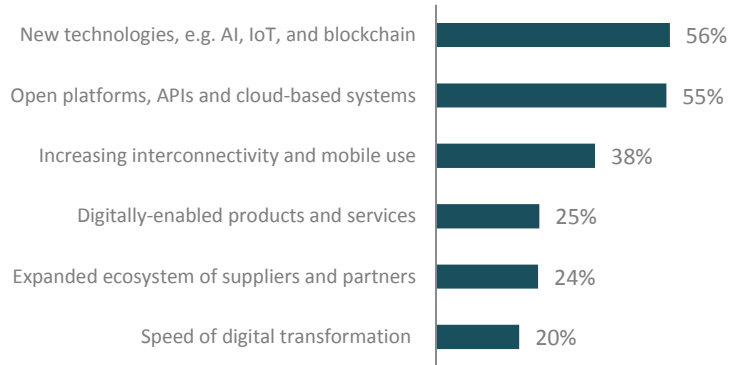
The risks from digital innovation

Digital innovation is a double-edged sword. While it improves business results, it also exposes companies to greater cyber threats as they embrace new technologies—such as AI and Internet of Things—and move to open platforms and cloud-based systems.

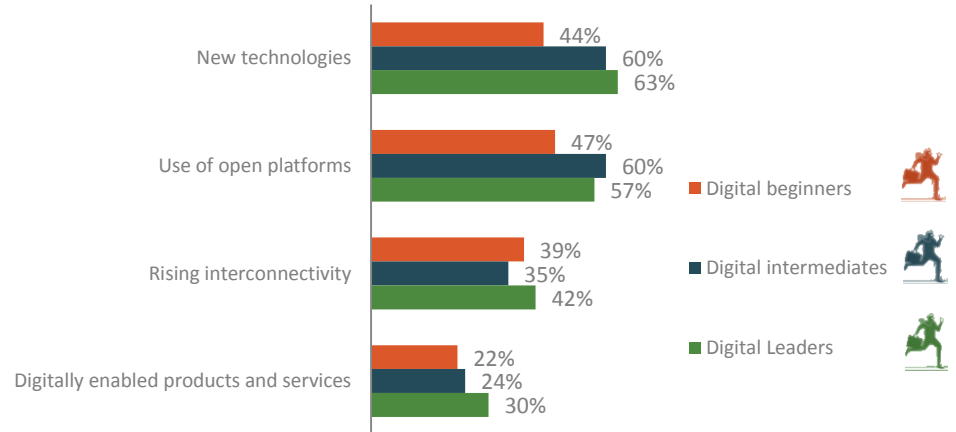
“As companies put everything on a digital platform and introduce IoT-operated devices, they create more attack points—which can have critical impacts on business beyond just personally identifiable information.”

Scott Laliberte, Managing Director, Protiviti

Impact of external and internal trends



Impact by stage of digital transformation



Which of the following external and internal trends are having the biggest impact on your cybersecurity risks and how you manage them?

The enemy within

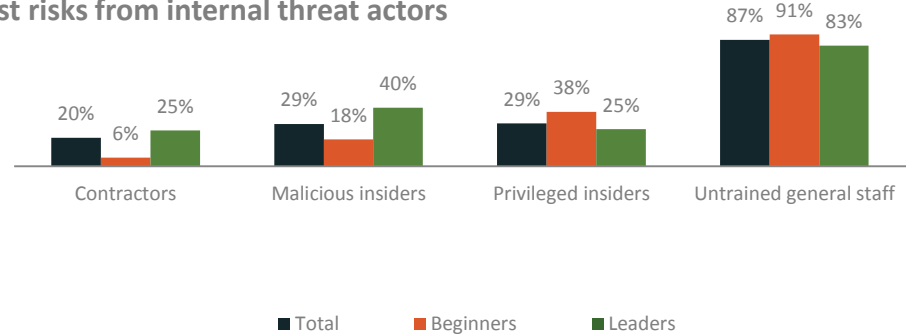
Nearly all firms (87%) see untrained general staff as the greatest cyber risk to their business because they may provide a conduit for outside attackers.

The next biggest threats are external: unsophisticated hackers (59%) and cyber criminals (57%). Surprisingly, most companies are less worried about government-sponsored hackers, with the exception of platform companies (10%). Cybersecurity beginners and leaders tend to have opposite views on the impact of both internal threat actors and external ones.

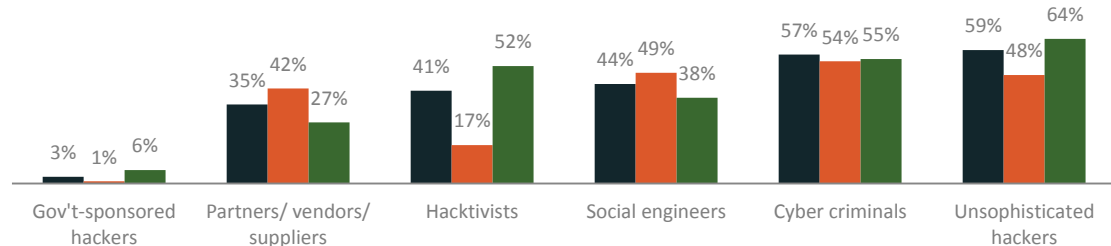
“People are absolutely the weakest link. Trying to convert everybody into a security professional is a losing proposition.”

David Estlick, CISO, Starbucks

Largest risks from internal threat actors



Largest risks from external threat actors



Which of the following parties create the largest risk for your business?

The dangers of ecosystems

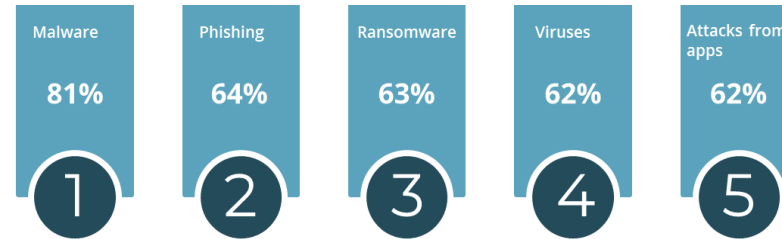
Although the most common attacks are now malware/spyware and phishing, the growing use of supplier ecosystems, embedded systems, and mobile and web applications will escalate risks.

Executives expect to see huge growth in attacks through third parties with network access (+247%), and also the reverse: attacks on partners and vendors through their own systems (+284%).

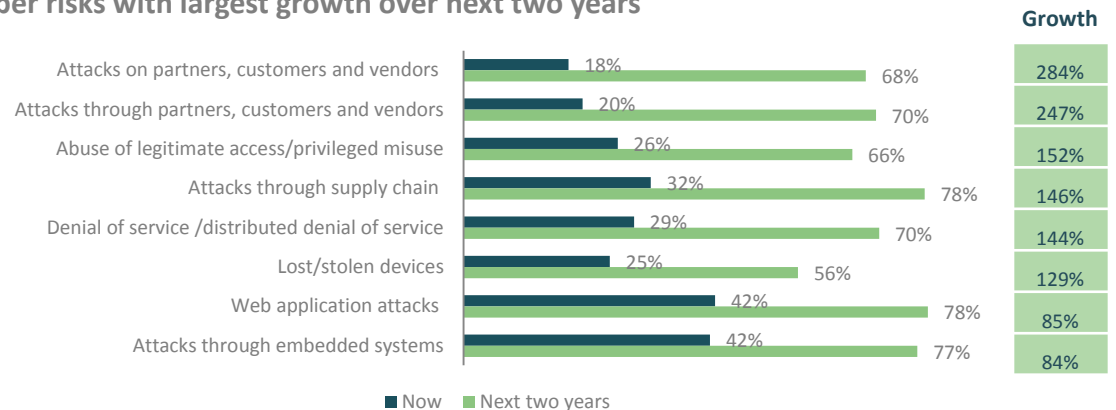
“Security issues driven by partners and suppliers are an ongoing concern.”

Larry Lidz, Global CISO, CNA Financial

Cyber-attacks with the largest impact on business today



Cyber risks with largest growth over next two years



Which of the following cybersecurity attacks are having the largest impact on your business now and which do you expect will have the largest impact over the next two years?

Where companies are vulnerable

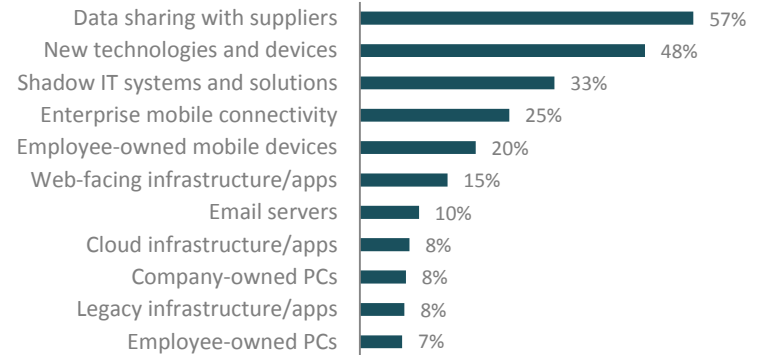


The growing complexity of IT infrastructure and connected devices is exposing firms to greater cybersecurity risks.

Data sharing is now the principal infrastructure vulnerability for most companies (57%). With integrated supply chains, energy companies and utilities (66%), consumer markets firms (60%), and manufacturers (58%) are the most susceptible. The use of new technology is the next major vulnerability (48%), followed by shadow IT, a particular area of exposure for IT-talent-rich platform companies (50%).

These top three vulnerabilities can sometimes be intertwined. Shadow IT, for example, often involves new technology and data sharing without oversight by enterprise security.

Greatest vulnerabilities across all firms...



...and in key industries



Data sharing with suppliers: Energy/utilities (66%), consumer markets (60%), manufacturing (58%), life sciences/healthcare (58%), and technology (57%)



New technologies and devices: Insurance (58%), and financial services (52%)



Shadow IT: Platform companies (50%)

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

Views on vulnerabilities



“A new piece of malware is released every day within 4.2 seconds. One of the problems that CISOs face is how to combat the sheer volume of malware bombarding us.”

Vali Ali, VP, Fellow, and Chief Technologist – Security and Privacy for Personal Systems, HP

“Although boards are paying more attention to cybersecurity, they are still underestimating the potential impact and threat.”

Brian Henesbaugh, Partner, Baker McKenzie



“If you look at the majority of breaches, 70-80% of them happened because of the lack of patches. Equifax is a classic case where they missed patching two services. Companies need to have a very strong patch program in place.” **Chintan Parekh, VP Cybersecurity, Fidelity**

“The number one way a hacker is going to attack a company is through social engineering: phishing or pretext phone calls. Number two is through exploiting vulnerable web applications, and number three is through compromising external network services.” **Kevin Mitnick, Chief Hacking Officer, KnowBe4**



The Road to Cybersecurity Excellence

“Great cybersecurity programs are not built in a month. They’re built over a span of years. You have to be willing to play the long game.”

Ron Mehring, VP, Technology and Security, Texas Health

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

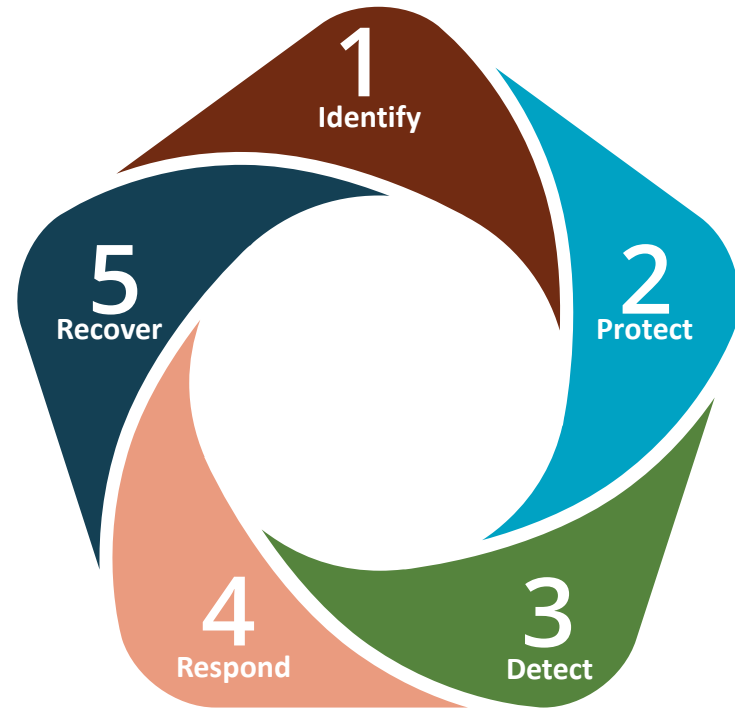
Using the NIST framework as a roadmap

The National Institute of Standards and Technology (NIST) and the International Standards Organization (ISO) are two common cybersecurity frameworks. While the nomenclature for these two standards is different, their goals are similar: to provide a roadmap to improving cybersecurity.

For our analysis, we used elements of the NIST framework to support our diagnostic survey tool. The survey questions were kept general so that respondents could provide answers regardless of which framework they use.

We asked executives to rate their company's progress across five key cybersecurity pillars: identify, protect, detect, respond, and recover. Based on these rankings, we created composite scores by industry, region, and other groupings. These scores reflect how companies in these segments fared against a mean score of 100.

In addition, we grouped companies into three categories based on the progress they have achieved against the five cybersecurity pillars: cybersecurity **beginners, intermediates, and leaders**.



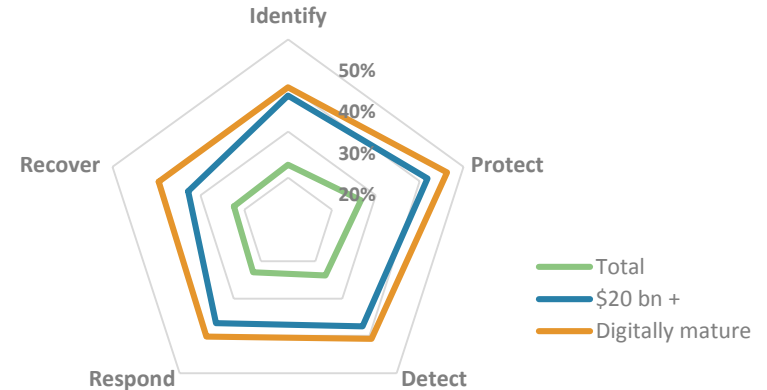
Cybersecurity: A work in progress

Based on our survey findings, just under half of companies (49%) are in the intermediate stage of cybersecurity maturity, while 31% are beginners and only 20% are leaders. So clearly there is considerably more that firms need to do to secure their business and customer information.

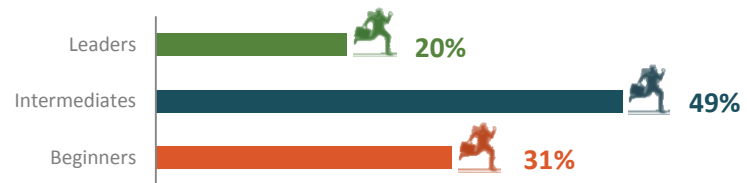
Most companies score highest on protect (27%) and detect (24%) and lowest on identify (23%), respond (23%), and recover (22%). Firms with revenue over \$20 bn and those in later stages of digital transformation have made more progress on key dimensions of cybersecurity.

While protection and detection are crucial parts of a balanced program—attackers are often not detected for long periods, which allows them to do more damage—these safeguards will not completely prevent hackers from breaking in. So companies would be wise to focus more on response and recovery.

Areas of greatest progress by category



% of firms by cybersecurity stage



What progress have you made in the NIST framework?

Aligning digital and cybersecurity maturity

Digital maturity often goes hand-in-hand with cybersecurity maturity—nearly 68% of digital beginners are cybersecurity beginners, and just 3% are cybersecurity leaders.

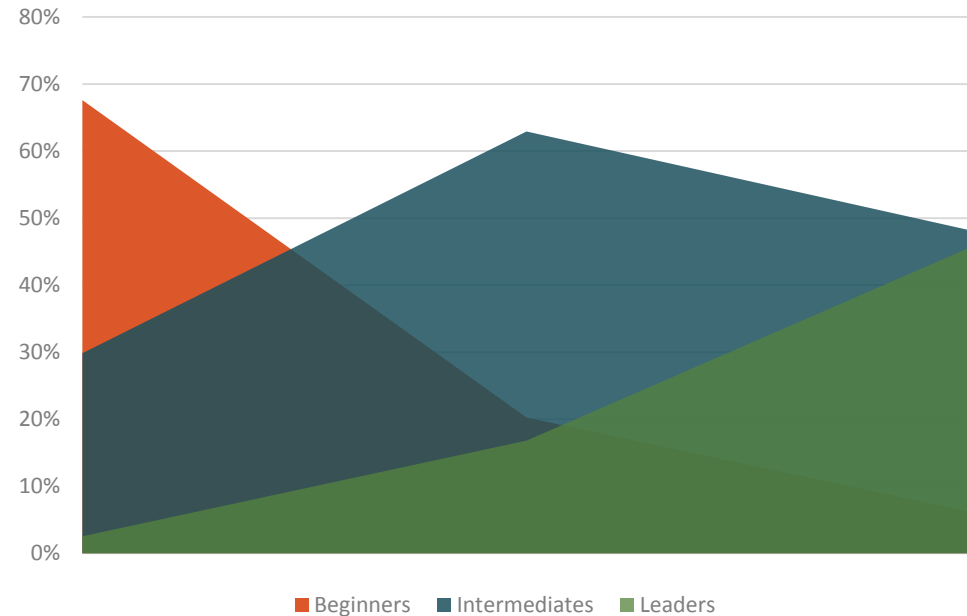
Unsurprisingly, 46% of digital leaders are also cybersecurity leaders; only 6% of digital leaders are cybersecurity beginners.

Nonetheless, a disconcertingly large number of digital leaders (over half) are NOT cybersecurity leaders, which leaves them more vulnerable to cyber attacks because of their higher reliance on digital platforms. To minimize risks, companies should build cybersecurity into each step of their digital transformation process.

“Digital innovation drives complexity and risks. A business leader can say, hey, I can use cloud services for everything. They’re not thinking about the legacy infrastructure or the continuity and backup necessary.”

Matthew Johnson, CISO, Willis Towers Watson

Cybersecurity maturity by stage of digital transformation



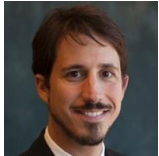
Views on where to focus cybersecurity efforts



“Financial firms are seeing increased focus on respond and recover due to pressure from the regulators. It’s not just about responding to a major cyber-attack. It’s ensuring the financial markets are functioning.” Jason Harrell, Executive Director, DTCC

“Companies should focus more on the beginning and end of the cybersecurity process. They should stop the hackers before they do damage, and know how to recover fast if they are unsuccessful.”

Patrick Moorhead, President, Moor Insights & Strategy



“Detecting and responding to security events is not easy, particularly as the bad guys get better at covering their tracks.” Larry Lidz, Global CISO, CNA Financial















“We’ve all seen breaches in recent years where companies got the response process wrong and seriously damaged their reputations. The GDPR 72-hour rule is also requiring firms to up their game in this area.”

Scott Laliberte, Managing Director, Protiviti



Progress against the NIST framework

While more than 80% of companies rate untrained general staff as the top threat actor, staff training is still one of the bottom NIST categories. Firms have made considerable progress on limiting access to physical assets; few companies (8%) cited this as a major vulnerability now.

| Top seven NIST categories | NIST functions | Bottom seven NIST categories | NIST functions |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| Limit access to physical and logical assets to authorized users and devices. | 39%  Protect | Prioritize the organization's objectives, stakeholders, and activities. | 18%  Identify |
| Analyze incidents to ensure effective response and support recovery. | 39%  Respond | Train staff and partners in cybersecurity awareness and to perform duties in line with policies and procedures. | 17%  Protect |
| Monitor information system and assets to identify cybersecurity events. | 36%  Detect | Identify data, data flows, devices, personnel and systems that could affect cybersecurity. | 16%  Identify |
| Maintain security policies and procedures for protecting information systems. | 35%  Protect | Perform maintenance and repairs of industrial control and information systems according to policies. | 14%  Protect |
| Manage data in line with risk strategy to protect integrity and availability of information. | 34%  Protect | Detect anomalous activity, understand the potential impact of events. | 13%  Detect |
| Establish priorities, risk tolerances, and assumptions. | 34%  Identify | Understand policies and processes to manage and monitor organization's regulatory, legal, risk, and operational requirements. | 11%  Identify |
| Identify cybersecurity risk to organizational operations and organizational assets. | 32%  Identify | Act to prevent expansion of an event, mitigate its effects, and resolve the incident. | 11%  Respond |

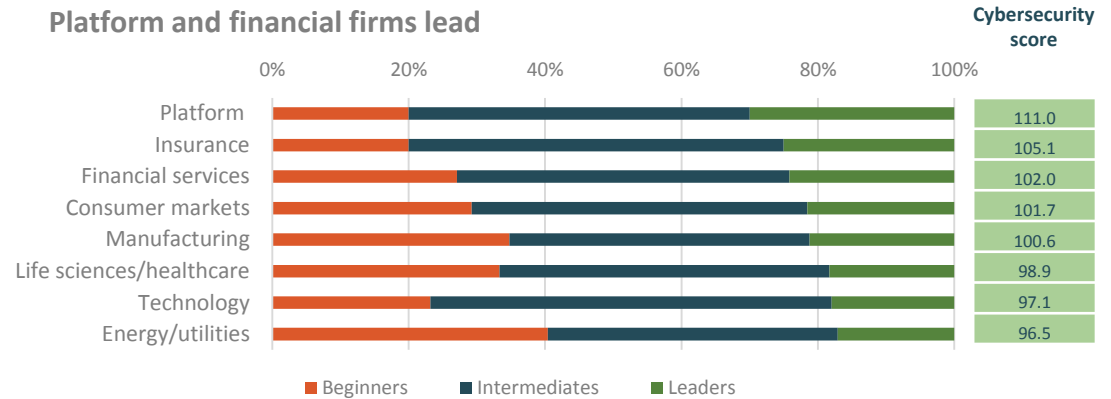
How firms stack up

To facilitate benchmarking, we developed cybersecurity maturity scores based on the progress against the five categories of the cybersecurity framework, with 100 as the average.

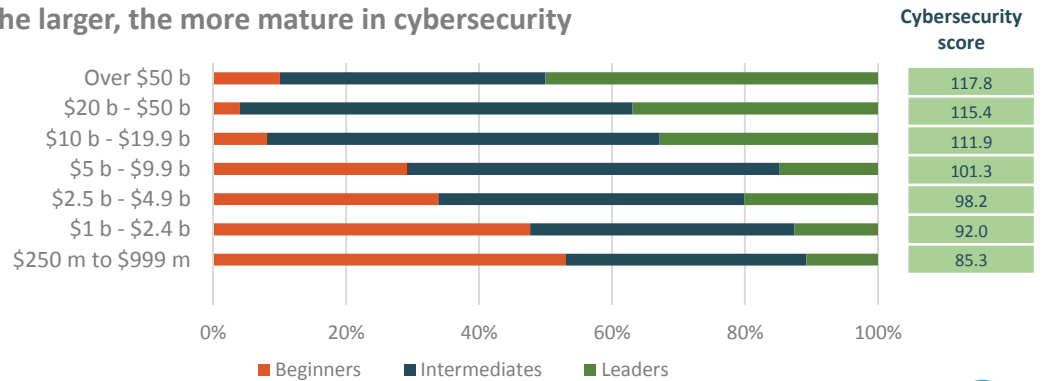
Platform companies are more likely to be leaders (30%) and have the highest cybersecurity maturity score (111), followed by insurance firms (105.1). Technology firms, which include smaller start-up organizations, are furthest behind.

The larger the company, the more advanced in cybersecurity. Companies with over \$50 billion in revenue have the highest cybersecurity score while firms with sales below \$1 billion have the lowest.

Platform and financial firms lead



The larger, the more mature in cybersecurity



Regional trends

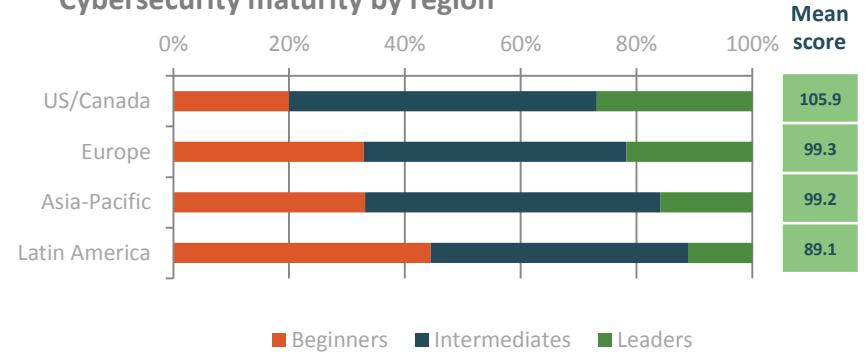
Cybersecurity maturity is highest in US/Canada, home to some of the world's most digitally advanced companies. US/Canada has the highest proportion of cybersecurity leaders (27%) and the top cybersecurity maturity score (105.9). Companies in US/Canada are ahead of firms in other regions for each of the five NIST categories, particularly in protection.

On the other end of the spectrum, Latin America has the fewest number of cybersecurity leaders (11%) and the lowest cybersecurity score of 89.1. Latin America lags behind other regions across all NIST categories, particularly in detection. The smaller size and global footprint of companies headquartered in Latin America contribute to that region's lower cybersecurity ranking.

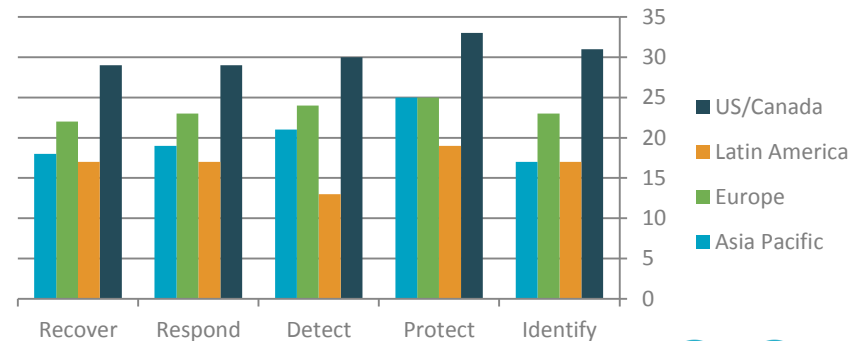
“More successful firms take a risk-based approach to everything: risk departments combine physical security and cybersecurity officers together.”

Joe Gittens, Technical Standards, SIA

Cybersecurity maturity by region



Progress against the NIST framework by region



Country scorecard

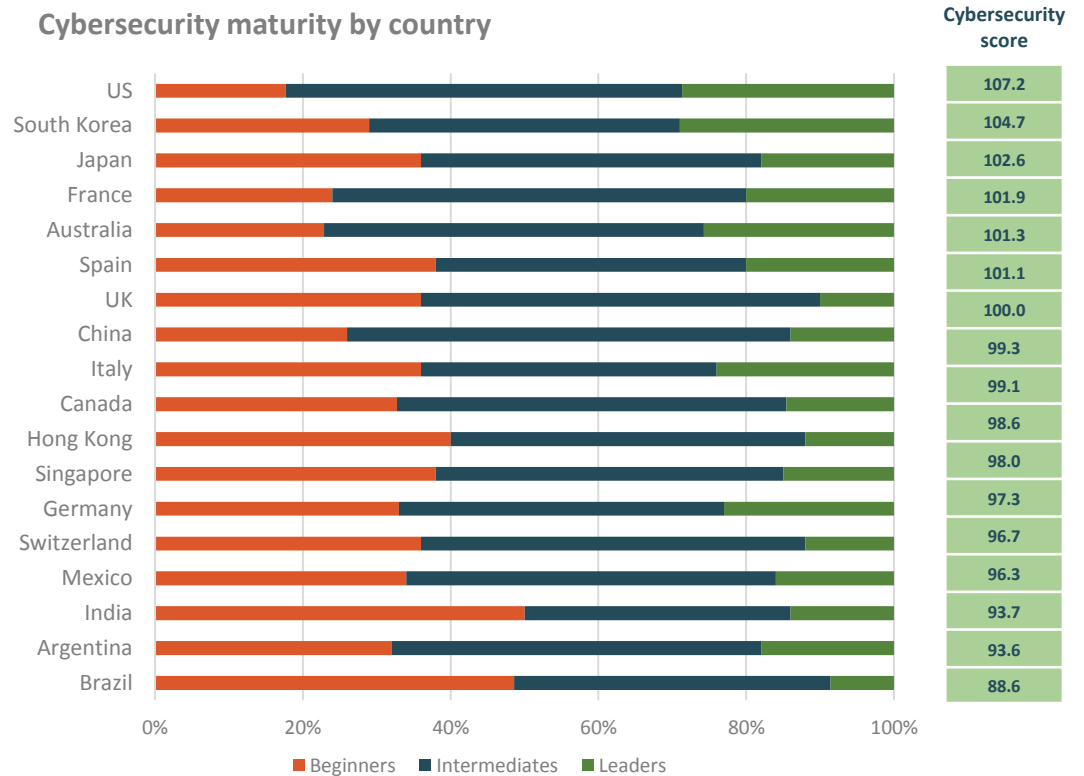
According to our analysis, the companies with the most advanced cybersecurity programs are in the US, South Korea, Japan, France, Australia, and Spain. These nations tend to be more digitally mature, and some, like South Korea, have major concerns about government-sponsored hackers. The firms furthest behind are in Brazil, Argentina, India, Mexico, Switzerland, and Germany.

With attacks coming from anywhere in the world, firms across countries need to step up their game to secure their businesses and customer data.

“In today’s global economy, everything is digitally connected. Whether it’s somebody in Russia, Nigeria, or China, they can carry out attacks quite effectively, from very far away.”

Brian Henesbaugh, Partner, Baker McKenzie

Cybersecurity maturity by country



Organizing for Cybersecurity

“Cybersecurity can be organized as a consultancy focusing on policy and process reporting to the general counsel or CRO, or as a service department aligned with the CIO or CTO. I prefer the latter, since it is more collaborative rather than adversarial.”

David Estlick, CISO, Starbucks

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Cybersecurity roles are fluid



Cybersecurity is still finding a home in many organizations.

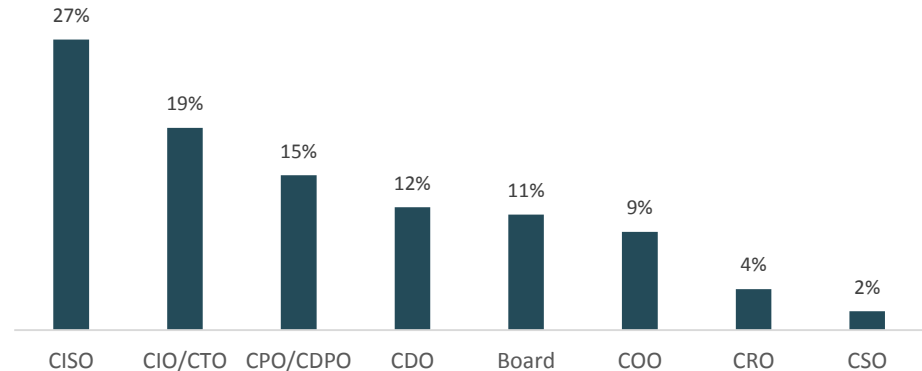
For over a quarter of firms, the CISO is responsible for cybersecurity, followed by CIO/CTOs (19%). Cybersecurity leaders are the most likely to assign responsibility to a CISO (37%), while beginners (23%) and companies with less than \$1 billion in revenue (26%) hold the board responsible.

The introduction of the EU's General Data Protection Law (GDPR), China's Cybersecurity Law, and other regulatory changes around the globe are giving rise to chief privacy officers (CPOs) and chief data protection officers (DPOs), who work collaboratively with CISOs and sometimes assume part or all of their roles.

"The CISO is one of those interesting functions – everybody thinks it's important, but nobody really wants it. It's the unwelcome person at the barbecue."

Matthew Johnson, CISO, Willis Towers Watson

Executive responsibility for cybersecurity

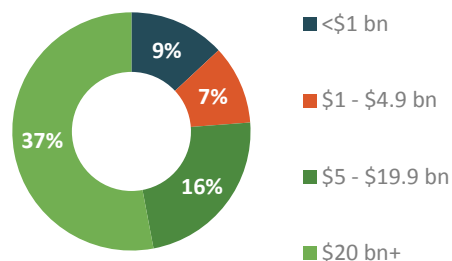


Which C-level executive is primarily responsible for cybersecurity risk management in your organization?

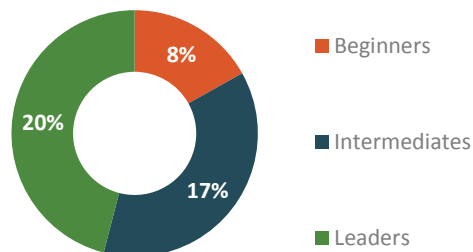
Privacy and security roles are coming together

Our survey shows that companies in Europe (20%) and the US/Canada (20%) sometimes give responsibility for cybersecurity to chief privacy officers or data protection officers (DPOs). The trend is more pronounced among \$20 billion-plus companies, and for data sensitive industries, such as consumer markets (18%) and life sciences/healthcare (17%).

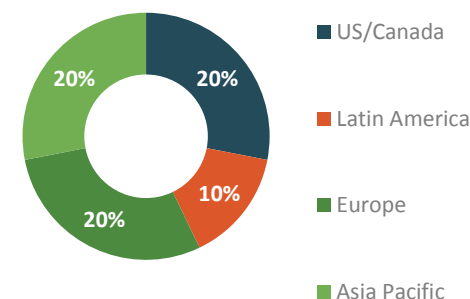
By revenue



By cybersecurity maturity



By regional HQ



Which C-level executive is primarily responsible for cybersecurity risk management in your organization?

14% of firms make chief privacy or data protection officers responsible for cybersecurity.

The rise of the data protection officer



“GDPR requires many firms to have a data protection officer. All of a sudden, you have an ombudsman for data privacy reporting to the board. There’s now a dichotomy between the IT-focused CISOs and the new customer-driven CDPO. That’s a big change, which companies need to address.”

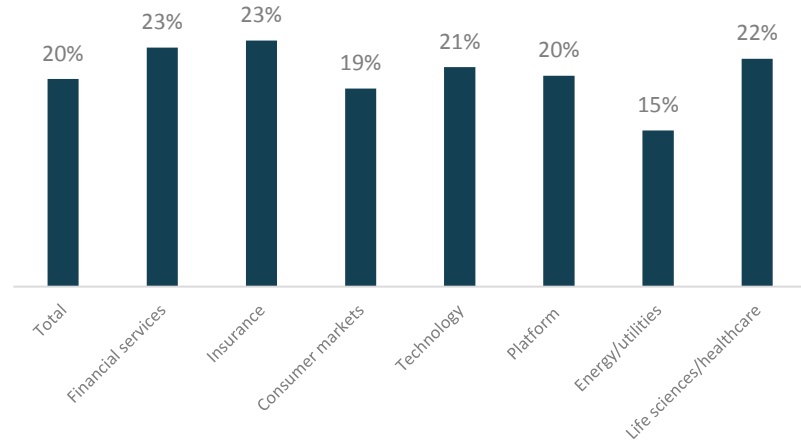
Mike Angle, CTO, Opus



“Under the GDPR, applicable firms need to be careful to avoid a conflict of interest when assigning the role of data protection officer (DPO). The role should be independent from the first line of defense.”

Tom Lemon, Managing Director, Protiviti

% of firms with a data protection officer (DPO) by industry



% of firms with a DPO by region



Staffing up for cybersecurity


The ratio of cybersecurity staff to technology staff and all staff vary widely by industry. Platform and technology firms have the highest cybersecurity staff ratios—more than 1 in three of tech staff-- followed by life sciences/healthcare, and manufacturing.

Ratios are lower for energy/utilities, financial services, insurance, and consumer markets companies. As more firms digitally transform their businesses, their ratios may move closer to those of technology and platform companies.

“Talent is critical. Without good talent, you risk not being able to have a best-in-class security program.”

Larry Lidz, Global CISO, CNA Financial

Cybersecurity staff ratios by industry

|  | Cybersecurity to tech staff | Cybersecurity to all staff |
|------------------------------------------------------------------------------------|-----------------------------|----------------------------|
| Platform | 1:2.8 | 1:90 |
| Technology | 1:2.9 | 1:22 |
| Life sciences/healthcare | 1:3.9 | 1:37 |
| Manufacturing | 1:4.6 | 1:45 |
| Consumer goods | 1:5.1 | 1:72 |
| Financial services | 1:5.3 | 1:44 |
| Insurance | 1:5.3 | 1:58 |
| Energy/utilities | 1:6.2 | 1:78 |

Approximately how large are your organization’s dedicated worldwide technology, information security, and cyber security staffs now? Please indicate the number of employees that work for your organization worldwide.

Cybersecurity staff ratios


Regional differences in cybersecurity staffing can be significant. Our results suggest that in APAC, cybersecurity staff is almost half the size of technology teams, although the ratio is 1:50 against all staff. Latin American companies trail in that ratio (1:8.3).

North American firms enjoy the highest ratio of cybersecurity to all staff (1:29). Other regions have cybersecurity: all staff ratios around 1:50. As companies expand their global operations, they tend to add slightly more cybersecurity talent.

There appears to be a correlation between staffing and performance results. For example, companies in the US/Canada have some of the highest staff ratios as well as cybersecurity scores. The reverse is true for Latin America.

Approximately how large are your organization's dedicated worldwide technology, information security, and cyber security staffs now? Please indicate the number of employees that work for your organization worldwide.

Cybersecurity staff ratios by region

|  | Asia-Pacific | US/Canada | Europe | Latin America |
|------------------------------------------------------------------------------------|--------------|-----------|--------|---------------|
| Cybersecurity staff compared to tech staff | 1:2.2 | 1:3.8 | 1:5 | 1:8.3 |
| Cybersecurity staff compared to all staff | 1:50 | 1:29 | 1:48 | 1:50 |

Cybersecurity staff ratios by level of internationalization

|  | 1 Region | 2-3 Regions | 4+ Regions |
|------------------------------------------------------------------------------------|----------|-------------|------------|
| Cybersecurity staff compared to tech staff | 1:4.5 | 1:4 | 1:3.8 |
| Cybersecurity staff compared to all staff | 1:53 | 1:34 | 1:36 |

As companies mature, cybersecurity staff ratios fall

While cybersecurity to total staff ratios stay constant as firms move up the cybersecurity maturity curve, the ratio of cybersecurity to technology staff drops.

One explanation: With better cybersecurity systems—and responsibilities dispersed throughout the enterprise—cybersecurity leaders need to hire fewer additional cyber-risk specialists. Another possibility is that more mature companies are outsourcing some of their efforts, particularly as they increasingly turn to cloud platforms and partner ecosystems.

As companies grow in revenue, economies of scale also come into play. Ratios to all staff drop as revenue rises, while ratios of cyber to tech staff peak in the \$1 to \$5 billion range.


“The industry is very short of cybersecurity talent. If you automate many of the lower-level tasks, you can use that limited talent for higher-level functions.”

Scott Laliberte, Managing Director, Protiviti

Cybersecurity staff ratios by cybersecurity maturity

|  | Beginners | Intermediates | Leaders |
|-------------------------------------------------------------------------------------|-----------|---------------|---------|
| Cybersecurity staff compared to tech staff | 1:3.6 | 1:3.7 | 1.48 |
| Cybersecurity staff compared to all staff | 1:40 | 1:42 | 1:40 |

Cybersecurity staff ratios by company size

|  | Under \$1 bn | \$1 - \$4.9 bn | \$5 - \$19.9 bn | \$20 bn + |
|------------------------------------------------------------------------------------|--------------|----------------|-----------------|-----------|
| Cybersecurity staff compared to tech staff | 1:4.4 | 1:3.3 | 1:3.6 | 1:4.4 |
| Cybersecurity staff compared to all staff | 1:22 | 1:32 | 1:40 | 1:45 |

Approximately how large are your organization’s dedicated worldwide technology, information security, and cyber security staffs now? Please indicate the number of employees that work for your organization worldwide.

Managing Cyber Risks

“Manage everything through a lens of risk. If you are managing through bad outcomes from incident to incident, you will never develop a sustainable program. A risk lens enables you to set agreed tolerances for prioritizing investments and allocating staff.”

Ron Mehring, VP, Technology and Security, Texas Health

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Cybersecurity through different lenses

While most companies regard cybersecurity as a financial, IT, and operational risk, some see its wider implications. As companies become more cybersecurity-mature, they look at InfoSec more as a reputational risk: 41% of leaders perceive this, versus only 19% of beginners. Leaders are also more apt to see the upside: cybersecurity as an enabler of digital transformation or an area of competitive advantage (23%), which only 6% of beginners believe. With the rise of GDPR, privacy officers are also more likely (20%) to see cybersecurity's competitive advantages.

How cybersecurity is viewed

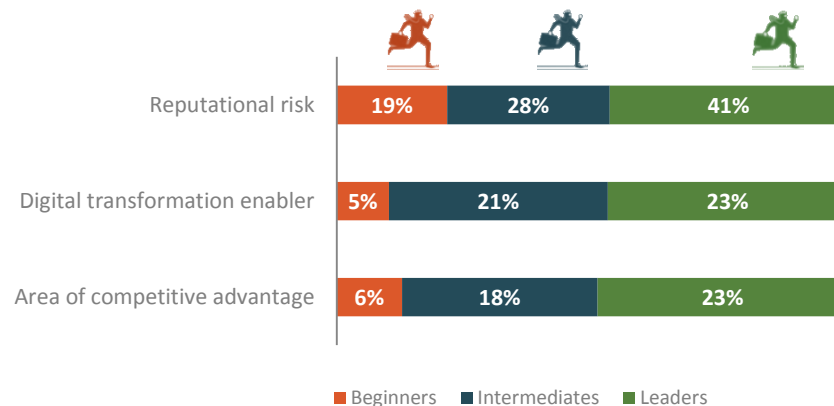


Enabler or enforcer?

25% of CEOs: digital transformation enabler

29% of CISOs and privacy officers: legal/compliance risk

Views change as a firm's cybersecurity approach matures



What are the main ways that cybersecurity is viewed in your organization?

Contrasting perspectives



“Cybersecurity means very different things to different people. Many firms are very early in their cybersecurity journey and don’t have processes or people yet. They are fighting to secure the infrastructure and educate internal users.” Vali Ali, VP, Fellow, and Chief Technologist – Security and Privacy for Personal Systems, HP

“To be successful in today’s marketplace, CISOs should enable the business to do new things safely. They can’t be traffic cops. They need to be enablers.” Dov Goldman, VP, Innovation, Opus



“Cybersecurity is no longer just a technology issue. It is now a USP (unique selling point) for financial firms. People prefer to work with financial organizations with the best security programs, where the data is secure.” Chintan Parekh, VP Cybersecurity, Fidelity

“People have been speaking of cybersecurity and InfoSec as business enablers for many, many years now. In my experience, it rarely steps up to that mark.”

Matthew Johnson, CISO, Willis Towers Watson



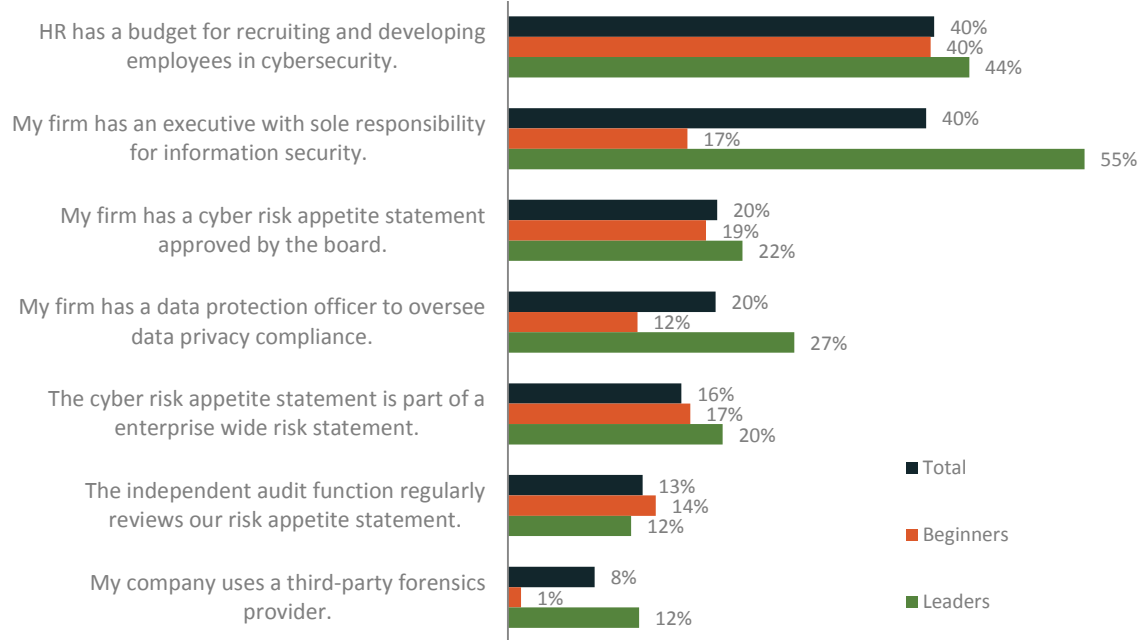
Cyber risk management approaches

4 out of 10 Have HR departments with budgets for recruiting and developing staff in cybersecurity and an equal number have executives who focus solely on cybersecurity.

2 out of 10 Have cyber risk appetite statements and a similar number have data protection officers in place.

<1 out of 10 Use a third-party forensics provider and even fewer define the materiality of a cybersecurity incident with a value.

As companies move up the cybersecurity maturity curve, their use of these approaches increases.



Which of the following statements apply to your organization's cyber risk management approach?

Insuring cybersecurity

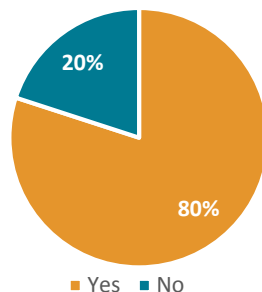
Most companies (80%) have at least a small amount of cybersecurity insurance. The larger the company and its global footprint, the higher its use of insurance.

More than 98% of insurance companies themselves carry cyber insurance, and they also tend to insure for the highest amounts (on average, \$16.5 million). Life science and healthcare organizations also hold large insurance policies (\$16.4 million), while manufacturing companies carry the least insurance (\$8.6 million.)

“Small and medium-sized businesses use cyber insurance far less than the Fortune 500: many believe they are not targets for cyber-attacks. But hackers don’t look for your particular company, just for a specific vulnerability.”

Michael Varshavski, VP Operations, CyberCube

Most companies have some type of cybersecurity insurance



Insurance coverage level by industry



| Industry | \$ millions |
|--------------------------|-------------|
| Insurance | \$16.5 |
| Life sciences/healthcare | \$16.4 |
| Technology | \$13.4 |
| Consumer markets | \$13.2 |
| Energy/utilities | \$12.9 |
| Financial services | \$12.7 |
| Manufacturing | \$8.6 |

Insurance by level of internationalization



| | |
|-------------|-----|
| 1 Region | 76% |
| 2-3 Regions | 73% |
| 4+ Regions | 90% |

Insurance by size



| | |
|------------------|-----|
| < \$1bn | 50% |
| \$1bn - \$4.5bn | 74% |
| \$5bn - \$19.9bn | 73% |
| \$20.0+bn | 97% |

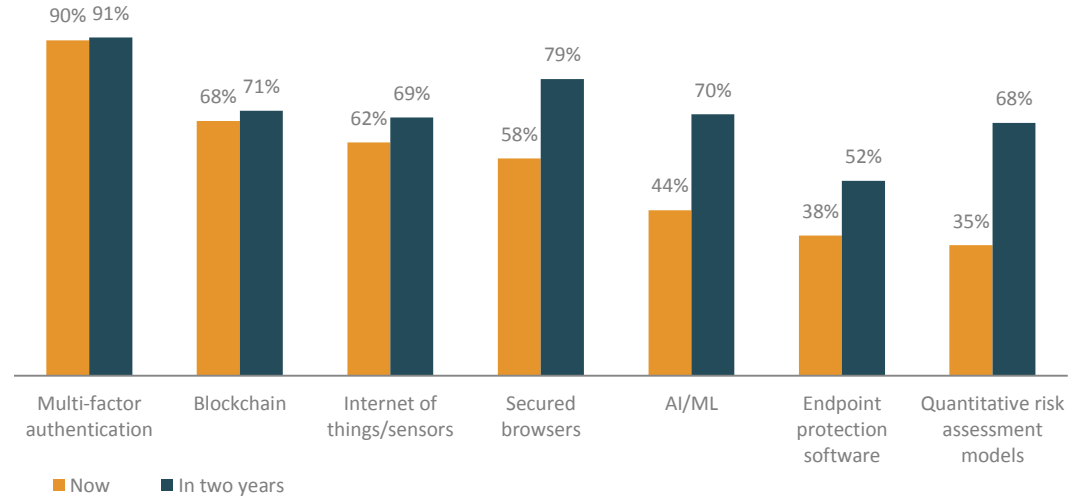
Does your company now hold cybersecurity insurance? If yes, how much is insured?

Tools of the trade

Companies will rely on a growing arsenal of cybersecurity technologies in the future. While multi-factor authentication is already table stakes (90%), other tools such as secured browsers and quantitative risk assessment models (FAIR) will grow to 79% and 68%, respectively, over the next two years.

Emerging technologies, such as blockchain and AI, which can improve cybersecurity, are also on the rise, particularly among very large companies. Blockchain use will climb to 71% in the future as more firms, especially in the financial, life science/healthcare, and technology industries, explore blockchain applications and the additional security they provide. During the same time period corporate AI usage will likewise jump—unfortunately it will probably also rise among the more skilled hackers.

Top technologies now and in two years



Which of the following technologies and IT services to manage cybersecurity risks is your company using now and which is your company planning to start using over the next two years?

“As IoT is adopted more broadly by companies, it will raise thorny security issues. In an interconnected world, every device purchase is a security decision.”

Vali Ali, VP, Fellow, and Chief Technologist – Security and Privacy for Personal Systems, HP

Fastest growing technologies

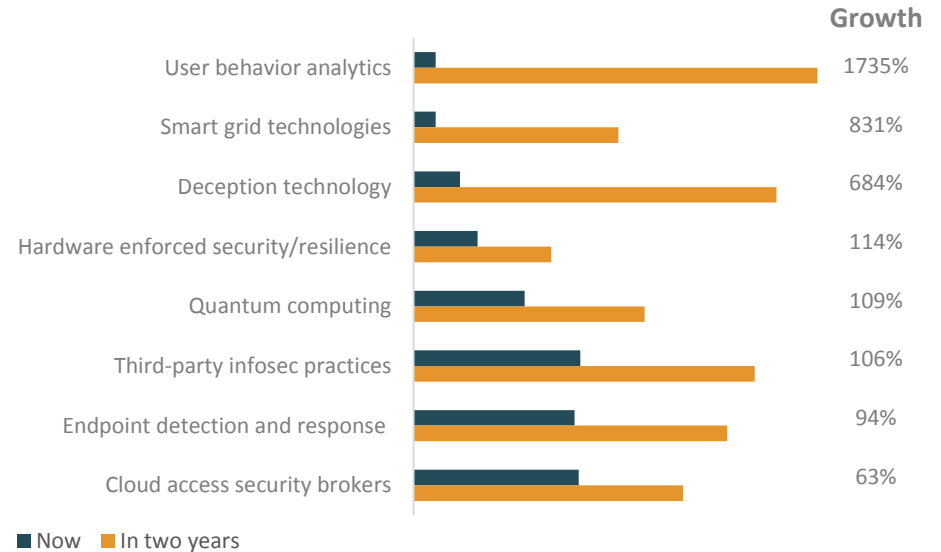
To help combat untrained general staff, today's biggest threat to cybersecurity, the fastest growing technology tool is user behavior analytics. Only about 4% currently employ it, but 73% plan to start using it over the next two years—a growth rate of more than 1,700%.

Smart grid technology (+831%), deception technology (+684%) are also slated to grow rapidly from a small current user base.

“We are using AI in our access and entitlement management to analyze the behaviors of end-users and determine whether or not their behaviors are risky.”

Ryan Fritts, CISO, ADT

Targeted to rise the most



Which of the following technologies and IT services to manage cybersecurity risks is your company using now and which is your company planning to start using over the next two years?

The Economics of Cybersecurity

“The board has to recognize that no organization is going to be 100% secure. It has to be willing to say on a scale of 1 to 10, we’re satisfied being a 7 because we realize for X amount of money, we can get to a 7. The board needs to decide on the amount of risk it is willing to accept.”

Scott Laliberte, Managing Director, Protiviti

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

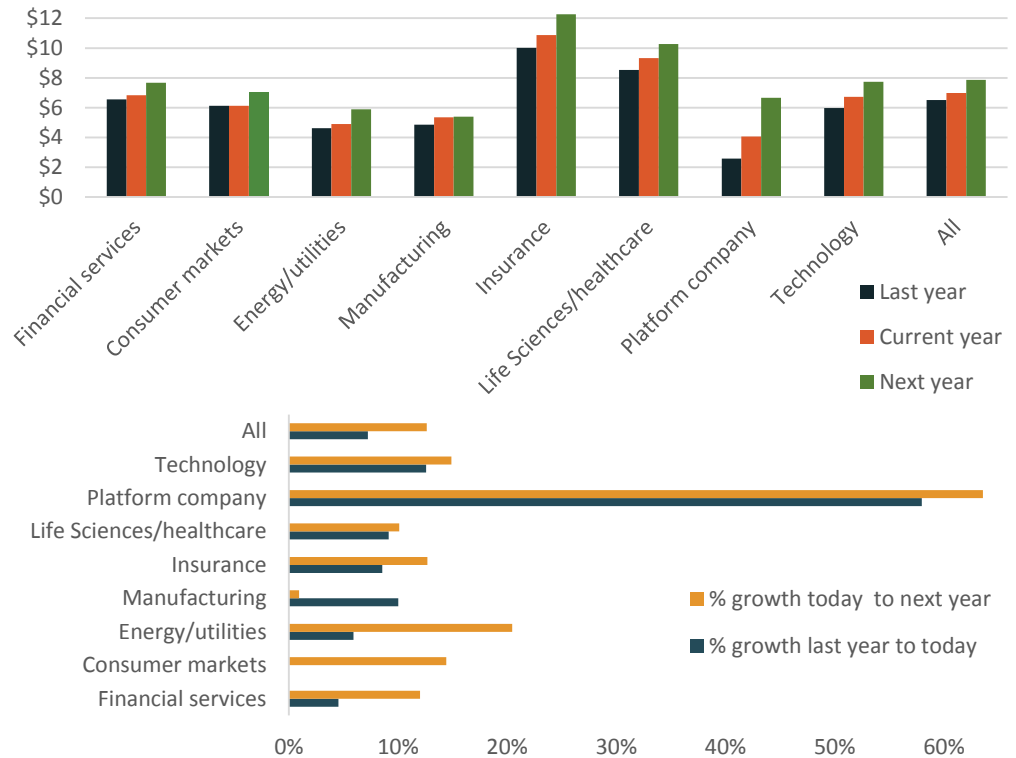
Companies are increasing their cybersecurity investments

To cope with rising cyber risks, companies increased their cybersecurity investments by 7% over the last year, and plan to nearly double that percentage increase to 13%. The biggest increases are by platform companies, which hiked their cybersecurity investment by 59% over the last year, and plan to increase their investment by a further 64% next year.

Smaller companies, whose cybersecurity systems are typically in early stages of development, will boost spending more next year: those with \$250m to \$1b in revenue (+33%); firms with \$1b-\$5b in revenue, +30%. Firms based in South Korea, which face some of the highest risks from government sponsored attacks, will increase their investment the most of those in any country, by 35%, with Mexico's close behind (+34%).

What investment did your company make in cybersecurity last fiscal year, and what investment is planned for the current and next fiscal year?

Average cybersecurity spending by industry (\$m and % growth)



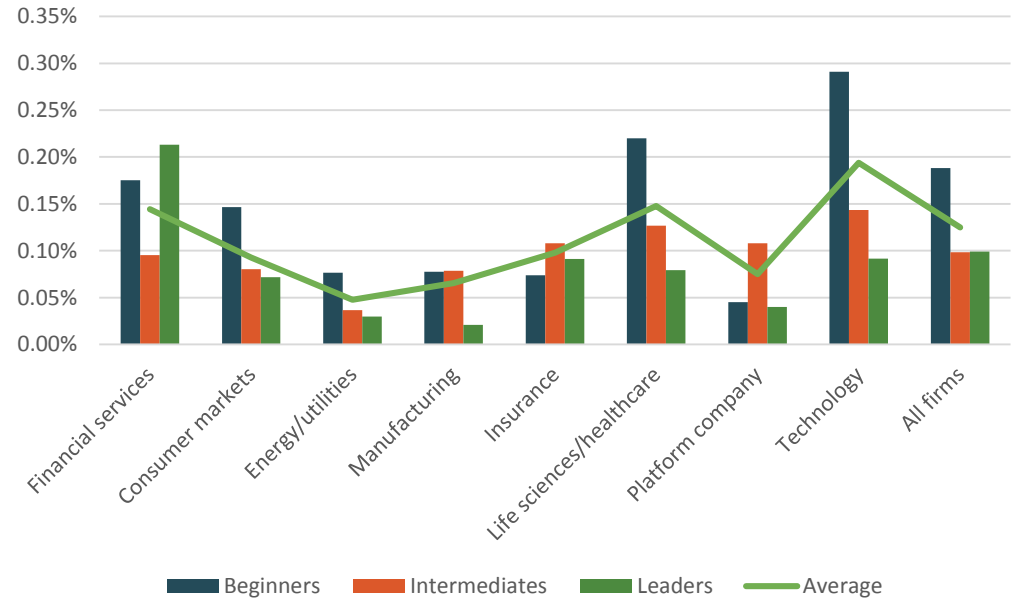
Cybersecurity spending declines as companies mature

On average, companies spend 0.1248% of revenue on cybersecurity—about \$12.5 million for a company with \$10 billion in revenues. On average, companies with revenue between \$250m-\$1b will spend \$2.8m next year, \$1b- \$5b (\$5.2m), \$5b-\$20b (\$9.6m), and \$20b+ (\$14.5m).

However, beginners spend more than firms further along the maturity curve. At face value, these results suggest that cybersecurity costs go down as firms become more advanced in their approaches and their ability to manage risk improves. This appears particularly the case for technology, life sciences, and financial services, which report some of the highest initial costs.

Our cybersecurity maturity analysis illuminates these spending patterns: 91% of cybersecurity leaders feel that their investment is adequate to meet their needs, while only 33% of beginning firms think that their investment is adequate.

Cybersecurity spending as a percent of revenue by industry and maturity



What investment did your company make in cybersecurity during the current fiscal year?

Protection will remain the chief area of investment



In the next year the budget for identify and detect will decline, and the amount for protect, respond, and recover will rise.

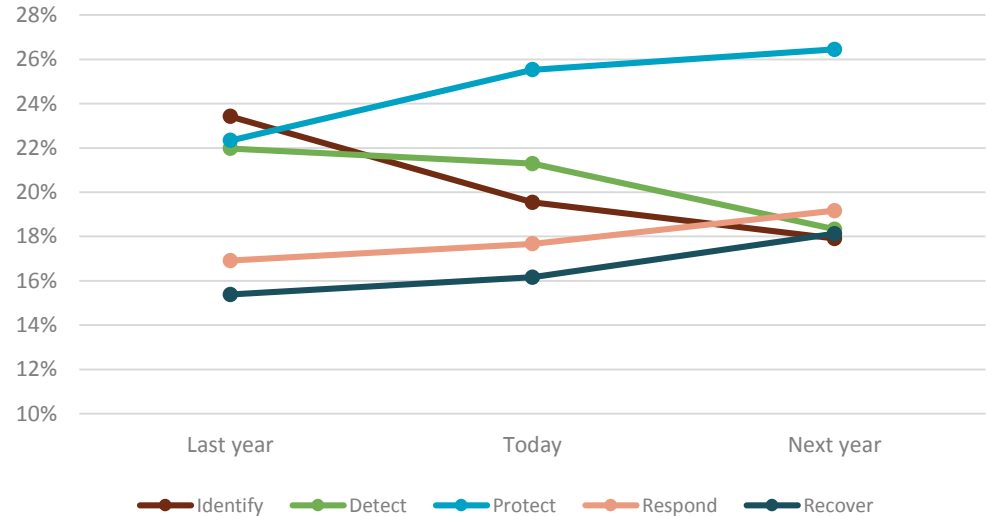
Our research shows that protection will continue to be the main focal point for investment across all industries next year (26%), with insurance companies spending the most (29%) and financial services the least (at 25%). Companies will also allocate more to respond (19%) and recover (18%) and less to identify (18%) and detect (18%).

Some experts suggest that this emphasis on protection is partly due to fear on the part of CISOs that they will be fired if there is a major breach. The lack of balance in investments may prove problematic in the long run.

“Prevention is better than cure. The more you can identify your risk upfront, the better for your firm.”

Chintan Jain, VP Security Engineering, Security Mantra

How spending on cybersecurity is evolving



What percentage of your cybersecurity budget is devoted to the five key cybersecurity functions identified by NIST? Please estimate for each time period.

Cybersecurity leaders invest more in resilience

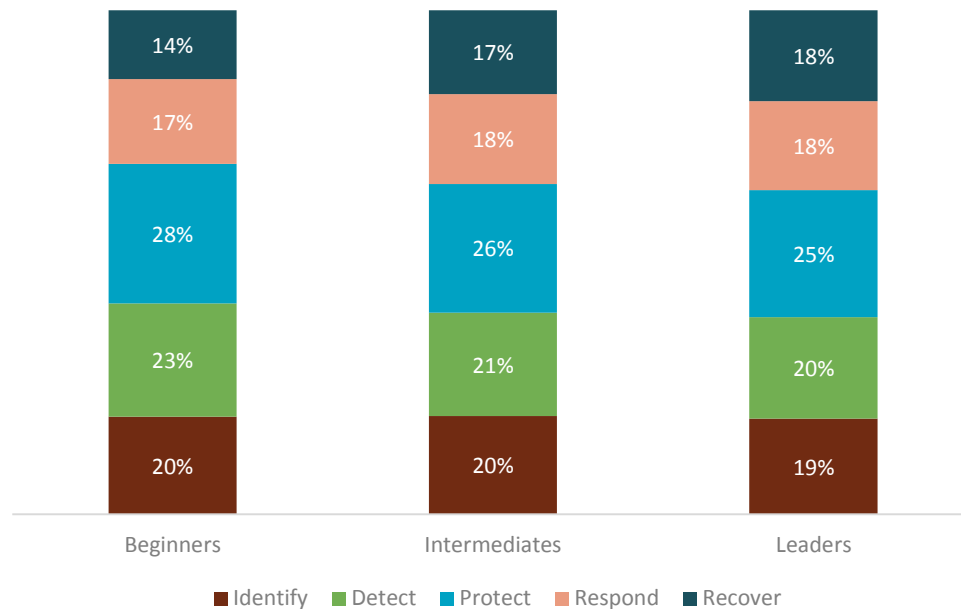
As they begin applying their cybersecurity frameworks, companies tend to invest mostly in protection, detection, and identification, and spend less on response and recovery.

However, as they become more advanced in cybersecurity, they increase their investment in response and recovery. For example, cybersecurity beginners are spending 14% on recovery for the current fiscal year, while leaders are spending 18%.

“You have to start with protection. But the biggest thing that the CISO needs to worry about is resiliency. How do I use people, processes, people and technology to drive detection and remediation?”

Vali Ali, VP, Fellow, and Chief Technologist – Security and Privacy for Personal Systems, HP

Cybersecurity spending by level of maturity



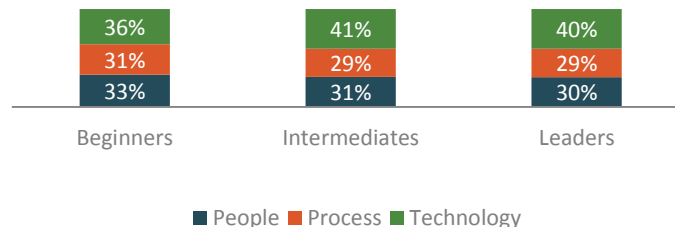
What percentage of your cybersecurity budget this year is devoted to the five key cybersecurity functions identified by NIST?

Balancing investment in people, process, and technology

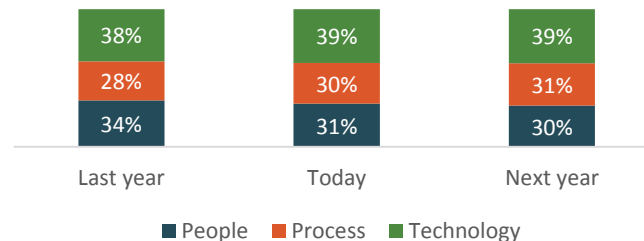
To win the “arms race” with hackers, companies last year allocated the largest share of their cybersecurity investments to technology (38%), followed by investments in people (including staff training) (34%) and process (28%). Next year, firms will increase their budget allocations to technology (39%) and process (31%), while trimming their allocation to people (30%).

While investment varies little by industry, it does change as cybersecurity maturity advances. Investing in people and process declines slightly, while technology spending grows. However, the lack of investment in automating processes could be a mistake—doing so could help compensate for the shortage of cybersecurity talent.

People, process and technology investment by maturity



People, process and technology investment over time



What percentage of your cybersecurity budget is devoted to people, process, and technology?

Cybersecurity beginners face the largest impacts

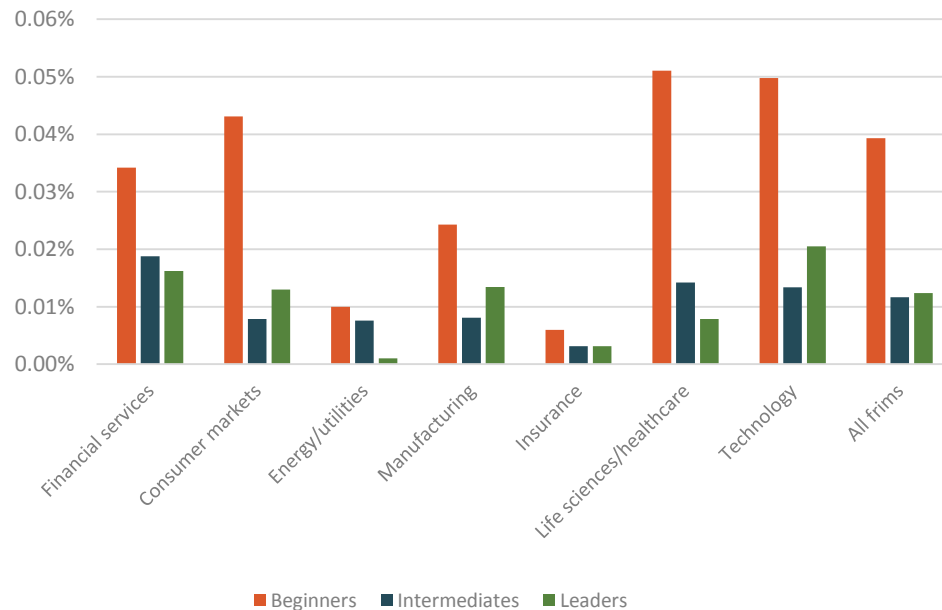


Across all industries, the cost of cyber attacks are highest at the outset

The higher impacts for cybersecurity beginners are most evident in certain industries: beginners in life sciences/healthcare and technology report higher costs—around .05% of revenue—than beginners in energy/utilities and insurance, where costs do not exceed those of intermediates and leaders by as large a margin.

Over the last fiscal year, what was your total cost for cyber loss events based on those factors that you measure?

Cybersecurity cost impacts as a % of revenue by industry and maturity



Measuring Cyber Risks

“It’s difficult to measure how well an organization is responding. Not only has the volume of attacks increased, but also the complexity and the sophistication of the attacks. It’s an ever-moving target.”

Brian Henesbaugh, Partner, Baker McKenzie

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Some industries are more vulnerable than others

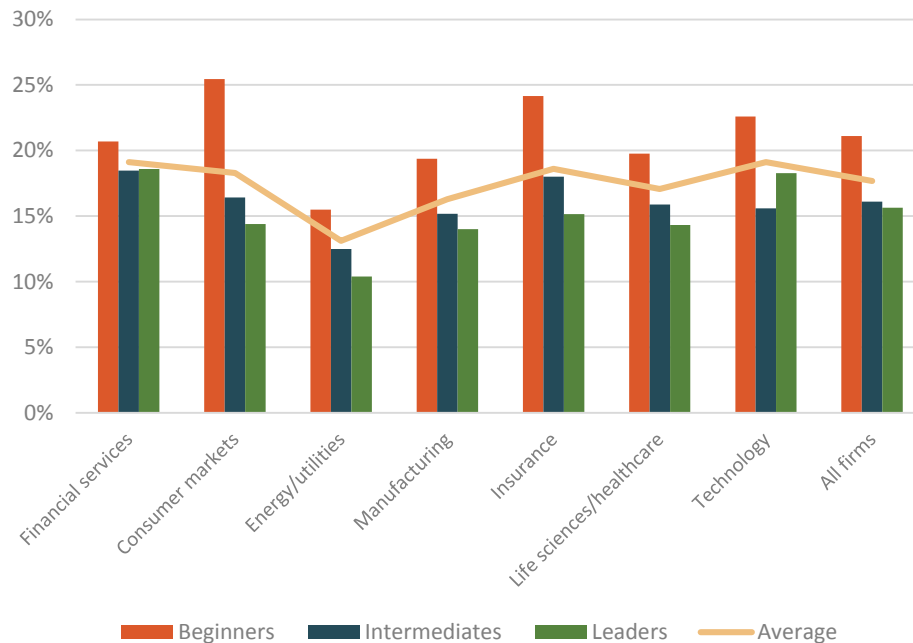
According to our survey, across all levels of cybersecurity maturity, financial services, insurance, and technology firms have the highest chance of suffering a successful cyber attack. The chances are particularly high for cybersecurity beginners in consumer markets and insurance. The chances are particularly high for cybersecurity beginners in consumer markets and insurance.

Energy firms and utilities have the lowest probability, particularly for cybersecurity leaders, which average just over a 10% probability, versus an average of 16% for more cybersecurity leaders across industries. The chances are higher for smaller companies, most likely because they tend to be less mature.

Chance of successful attack by company size (revenue)



Chance of successful attack by industry and cybersecurity maturity



Probability of having more than \$1 million in losses from a cyberattack next year.

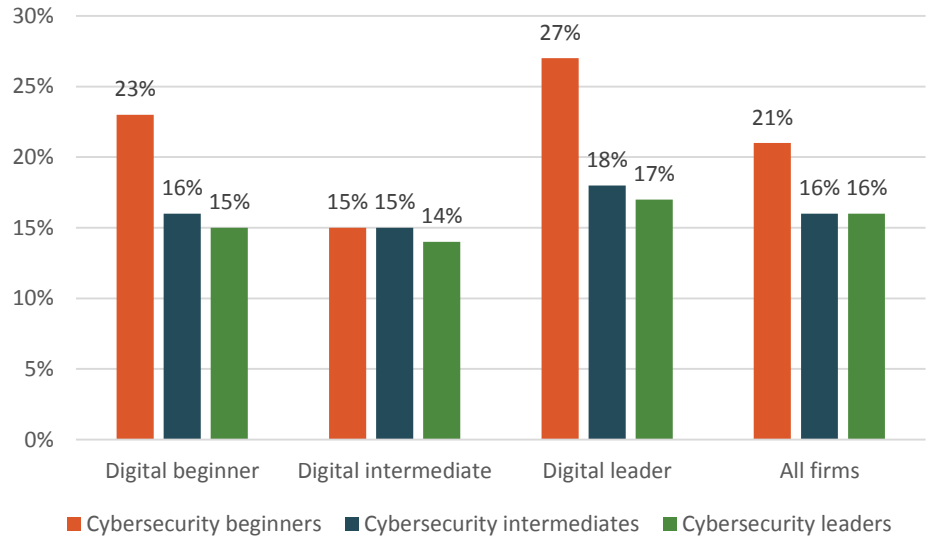
Cybersecurity beginners are more vulnerable to attacks

Across all firms, cybersecurity beginners have a higher probability of suffering a successful cyber-attack that results in more than \$1 million in losses—about 21%, while for cybersecurity intermediates and leaders, the average is 16%.

Our analysis shows that the likelihood of a loss event generally rises for most companies as they digitally transform their businesses. That is why it is crucial for companies to ensure cybersecurity maturity keeps pace with digital transformation.

One case in point: Cybersecurity beginners have a 23% chance of having more than \$1 million in losses when they are in the early stages of digital transformation. But if they do not improve cybersecurity in line with digital transformation, then the likelihood rises to 27%.

Probability of having more than \$1 million in losses

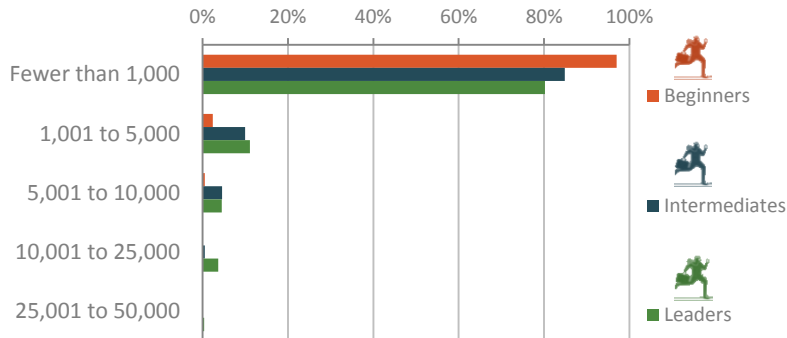


Probability of having more than \$1 million in losses from a cyberattack next year.

Why do firms see more attacks as they improve cybersecurity?

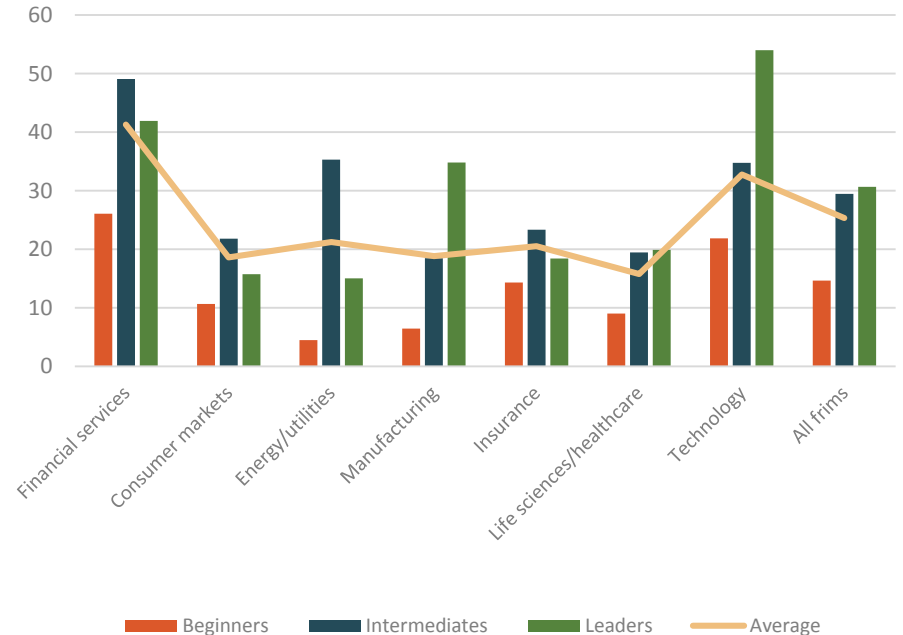
While firms believe that the chance of a successful attack falls as they advance in cybersecurity maturity, our analysis shows otherwise. Cybersecurity beginners, regardless of sector, report fewer successful attacks per year than companies that are more mature in cybersecurity maturity. They also report fewer customer records lost or stolen than more mature companies do. There are two possible explanations: the speed of digital transformation or poor detection.

Number of successful attacks by maturity



Please provide us with information on the following cybersecurity performance metrics used for external, customer-facing activities.

Number of incidents by industry and maturity



Over the last fiscal year, on average, how long was it between cybersecurity incidents?

Digital transformation or poor detection?

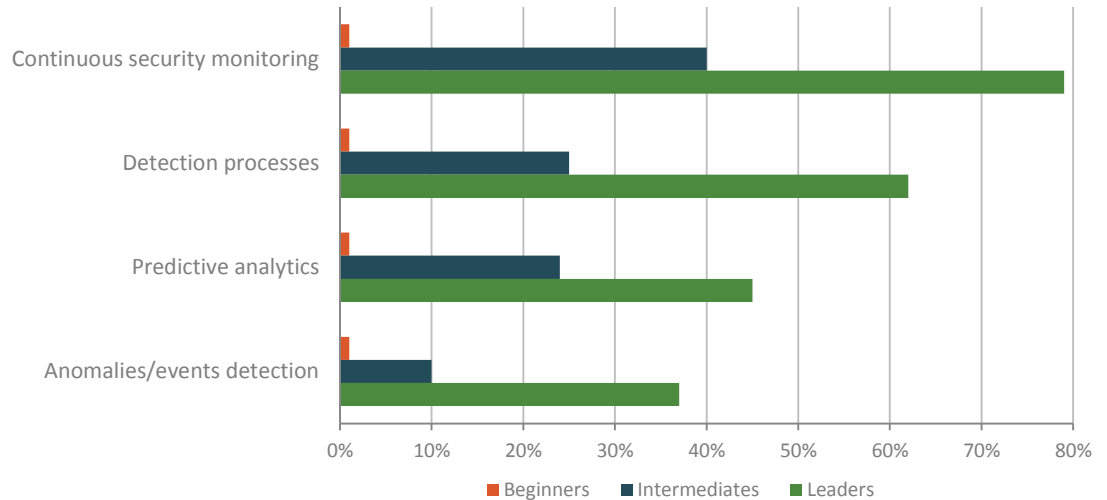
One reason for this anomaly is that the speed of digital transformation can expose companies to greater cyber risks if cybersecurity programs do not keep pace.

But the most likely explanation is that cybersecurity beginners are under-reporting their cyber attacks. Only a tiny percentage of beginners have made significant progress in setting up effective detection systems: for example, only 1% have made progress in continuous security monitoring, while 40% of intermediates and 79% of leaders have done so. As a result, they may simply be unaware that they have been breached.

What progress have you made in each of the following activities to DETECT cybersecurity risks? (Top two stages)

“Security is not typically the priority for teams digitally transforming businesses and products. They end up creating products with many risks, then bring in security at the last moment, when it is too late to fix them.” Chintan Jain, VP Security Engineering, Security Mantra

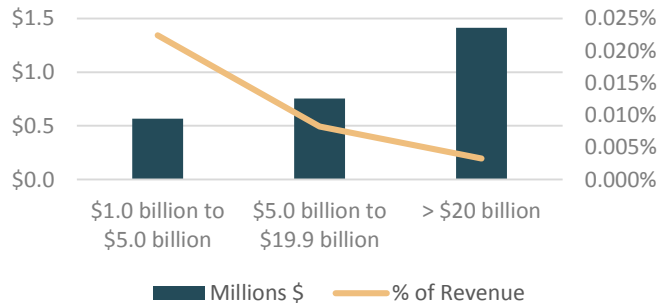
Progress in key areas of cyber risk detection



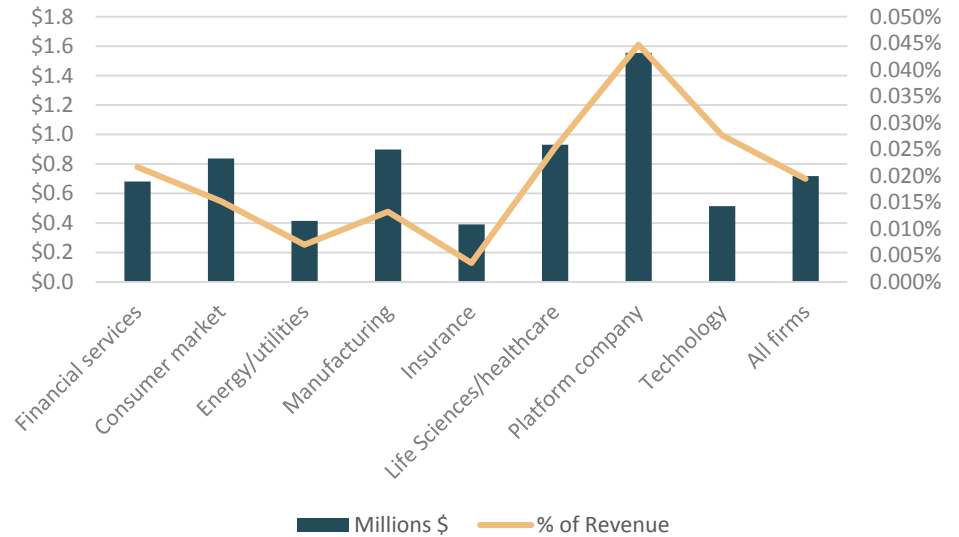
The costs of cyberattacks vary by industry and size

The costs of cyberattacks is highest for platform companies—which are major targets for hackers—both in dollar terms and as a percentage of revenue; more than double the average. Life sciences/healthcare companies also lose more than average from attacks in both dollar and revenue terms, and tech firms pay more than average as a percentage of revenue. Insurance companies and energy/utilities are the best off, with losses below average on both measures. Costs decline as a percentage of revenue as company size increases.

Cost of cyberattacks by company size (revenue)



Cost of cyberattacks by industry

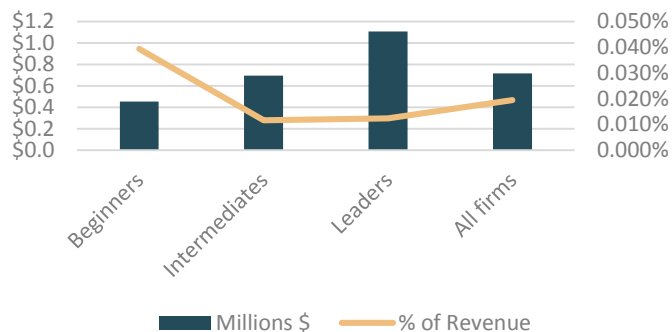


Over the last fiscal year, what was your total cost for cyber loss events based on those factors that you measure?

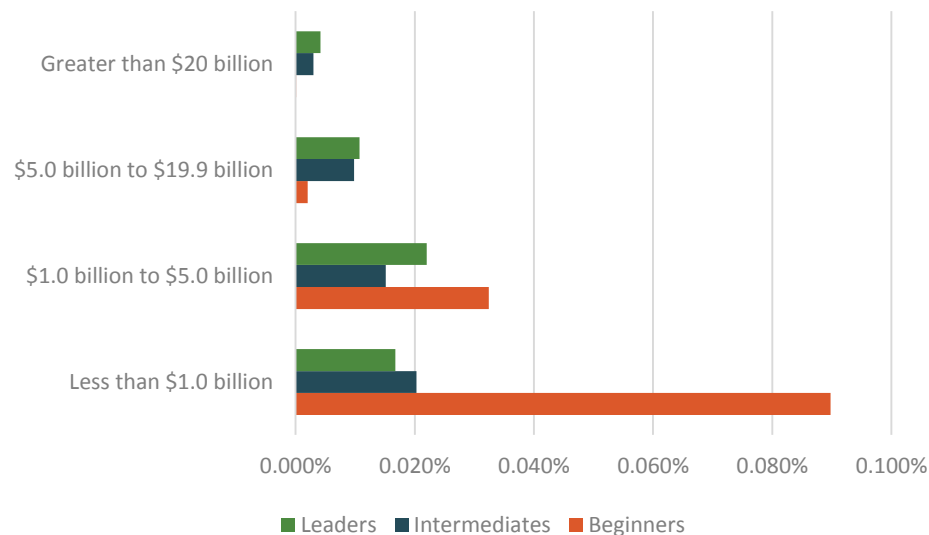
The costs of cyberattacks fall as maturity increases

Not only does the probability of cyberattacks decline as companies mature in cybersecurity, so do the costs. These are highest for beginners (0.039% of revenue or \$4 million for a \$10 billion company) more than triple those of leaders (0.012% of revenue for leaders, or \$1.2 million for a \$10 billion company). And costs for beginners may be even higher, since they are likely underestimating the costs due to their ineffective detection systems.

Cost of cyberattacks by cybersecurity maturity



Cost of cyberattacks by size and maturity



Over the last fiscal year, what was your total cost for cyber loss events based on those factors that you measure?

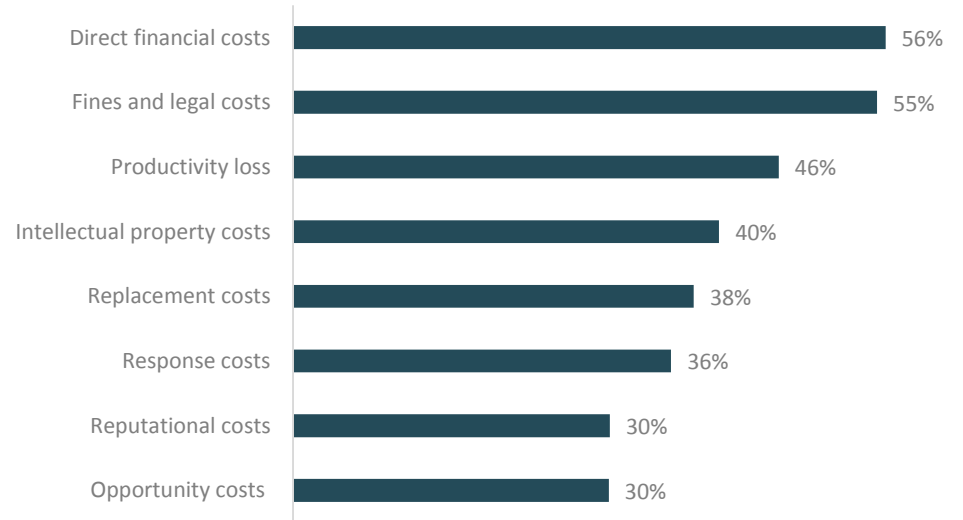
How the costs of cyber attacks break down

Cyber attacks are expensive for companies in both direct and indirect ways. The two largest costs resulting from cyber attacks are direct financial losses and expenses, such as theft and compensation of victims, and fines and legal penalties.

Firms are more likely to measure the costs that involve actual dollars, such as the direct financial costs, replacement costs or fines and legal costs. Nearly all survey respondents measure these costs.

However—likely because they are so hard to quantify—fewer companies measure indirect costs. Some 11% of companies do not measure productivity loss, 20% do not measure opportunity costs, and 21% do not measure reputational costs, all of which could prove more expensive in the long run.

Costs of cyber attacks with the highest impact



How did each of the following types of cyber incident losses impact your business over the last fiscal year?
(Showing high or very high impact)

Calls to Action

Cybersecurity is still more of an art than a science. So we spoke to CISOs, cybersecurity experts, technologists, and even former hackers, to learn more about the state of the art. To get a balanced perspective, we interviewed leaders across industries. Here is what they advise.

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Calls to action



1. Build a cybersecurity roadmap

"Start by tying your cybersecurity risk program to the enterprise risk management process, so that it's not just IT and security people driving the risk assessment. Put in an effective governance structure that has representation from the business and the other key stakeholders.

Next, right-size the cyber program to match the risk profile and appetite of top management. Remember that technology alone doesn't solve the problem—you need to have the right people and process to support it. Regularly test your detection and monitoring capabilities to make sure they are effective.

Finally, develop key metrics so you can ensure you're achieving your goals, and develop a feedback loop to refine the program as it goes along."

Scott Laliberte, Protiviti



2. Conduct an audit

"The first thing I would do is to have a third-party audit firm baseline my current services against those of my peers, so I can identify those areas where I need to strengthen my security to at least draw even with the herd.

That would help me figure out which programs I need to implement immediately. If I'm a medium-sized firm, I would do that in addition to looking at how I stack up against the NIST cybersecurity framework. Regulators are looking more and more to that framework and asking: 'Have you measured yourself against this? If you did, where do you stand?'"

Jason Harrell, DTCC

Calls to action



3. Look at cybersecurity through three verticals

"The first is the advisory side. Make sure you've got everything buttoned down – from tone at the top through to product design. The next vertical is transactional. What are the cybersecurity and privacy issues relating to engagement with suppliers and customers? Lastly is crisis and disputes. Prepare a really solid response policy that's going to be well practiced among the core and ancillary team, including notification duties, forensics, law enforcement, PR and preparing for class actions."

Brian Henesbaugh, Baker McKenzie

5. Invest in a cybersecurity culture

*"Culture is crucial: you need to develop an information security culture that is part of every single thing you do. It can be your best line of defense. **Mike Angle, Opus***



4. Walk before you run

"We think of cybersecurity as a very complex subject, but a lot of time it is just common sense. Rather than focusing on many advanced technologies to secure, first make sure you are doing the fundamentals right."

Chintan Parekh, Fidelity



Calls to action



6. Get buy-in from the top

"Effective cybersecurity and compliance starts at the top. The Board and the CEO set the tone for governance, funding and behavior – and without their ownership and sustained support the cybersecurity program will fail."

Lee Kirschbaum, Opus



7. Ensure access is secure

"You have to have a robust, auditable, impeccable access control system so that you know all the time who has access to all your critical systems. We have dual authentication for everything. There are other ways to do it as well, but just having a simple password and no other requirements and saying you are protected, is not a best practice."

Michael Varshavski, CyberCube



8. Change how you communicate

"One of the challenges for us as security professionals is that we talk a different language. We find it very difficult to relate to business speak—instead, we talk about cost avoidance: 'If you don't do this, these things will happen and cost this, or we will fail the regulator's test and be fined.' We don't frame the discussion in business terms: if we do this, you can reduce your time to market for new products."

Matthew Johnson, Willis Towers Watson

Calls to action



9. Adopt a proactive mindset

“Just implementing a set of tools to help find things puts you in a reactive position. You need to take a proactive stance in managing your security program by starting with the mindset that you have been compromised and set out every day to disprove it. You might be using the same tools, but how you go about executing on them will be very different.”

Ryan Fritts, ADT



10. Assume a breach

“If you’re not proactive, the bad guy is always going to get in. You might be proactive, and he still might get in. You have to make an assumption of breach and remediate as soon as possible. For example, if the company realizes an endpoint was infected with malware, they should seriously consider reloading that machine from a known good source.”

Kevin Mitnick, KnowBe4



11. Don’t manage cyber and physical security in silos

“Security is a holistic discipline. You need to manage both physical and cyber risks. You could have the best physical security ever – guards, gates, guns, surveillance – but if someone can access your network from the comfort of their living room, it’s not doing anything. The reverse is true as well. You could have a ton of cybersecurity, but fail to fully lock down your physical space.”

Joseph Gittens, SIA

Calls to action



12. Shift your focus to people and devices

"Securing your network perimeter is no longer enough. The office of the future is very different: people are working from anywhere and everywhere—when they are at Starbucks, on vacation, in transit or sitting at home. The peripheral boundary of your network is simply not strong enough to protect inflows and outflows of information.

CISOs need to shift their attention to users and their devices. Too often, the devices are the last part of the thought process, when they should be the first. These devices may stay in your organization for years, and their defenses may go bad or may not be automatically updated. Every device purchase is a security decision."

Vali Ali, HP



13. Don't make cybersecurity an afterthought

"When creating digital products, companies need to build security into those products from the get-go, rather than securing them after they are built. Right now, most firms have cybersecurity siloed in one organization, which might have 5% of the staff of the engineering group. When one of these engineers creates a product, they then look to cybersecurity to do some penetration testing to secure the product.

But the cybersecurity group doesn't have the time because they are already so overwhelmed with other requests. The staffing is not there. And often, once the product is developed, it's too late to fix all the issues. You need to have cybersecurity people embedded in the teams that are creating products and digital transformation."

Chintan Jain, Security Mantra

Calls to action



14. Ensure your personal success as a CISO

"First, make sure you're a continuous learner. You shouldn't be in security if you're not inquisitive. It's a fast-paced environment that requires people who have a thirst for knowledge and learning.

Second, build an organization that delivers value. You should be able to come back and say these are the services that I provide for my organization. It is not just thoughts, opinions, and process.

Lastly, position yourself appropriately within your organization. Set the expectations with your leadership and your peers. Let them know first and foremost your role is to support the business."

David Estlick, Starbucks

Research Background

[Introduction](#)

[Executive Summary](#)

[Evolving Risk Landscape](#)

[Road to Excellence](#)

[Organizing for Cybersecurity](#)

[Managing Cyber Risks](#)

[Economics of Cybersecurity](#)

[Measuring Cyber Risks](#)

[Calls to Action](#)

[Research Background](#)

[Acknowledgements](#)

Research methodology

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

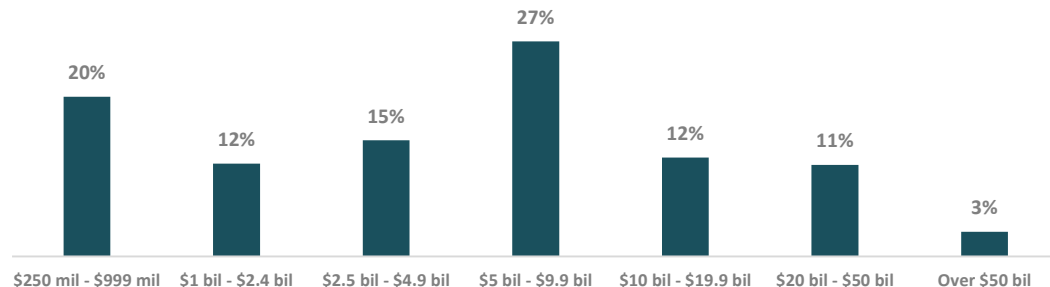
1. Cross-industry survey of 1,300 worldwide executives with insights into their companies' cybersecurity approaches and results.
2. Consultation with an advisory board of experts and practitioners from leading organizations with varied perspectives on cybersecurity.
3. In-depth interviews with CISOs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



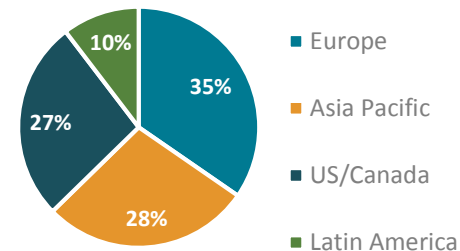
Survey: Respondent profile

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

Revenue



Region



Ownership type*



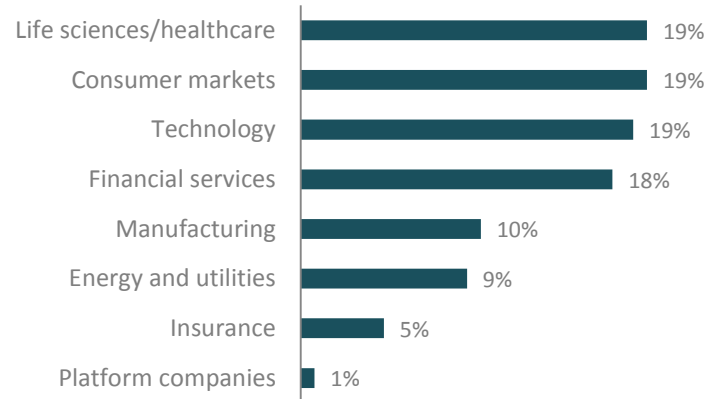
*Percentages rounded to nearest whole number

In which country is your company based? What were your company's revenues (in US dollars) in your most recent fiscal year? Please describe your organization's ownership type.

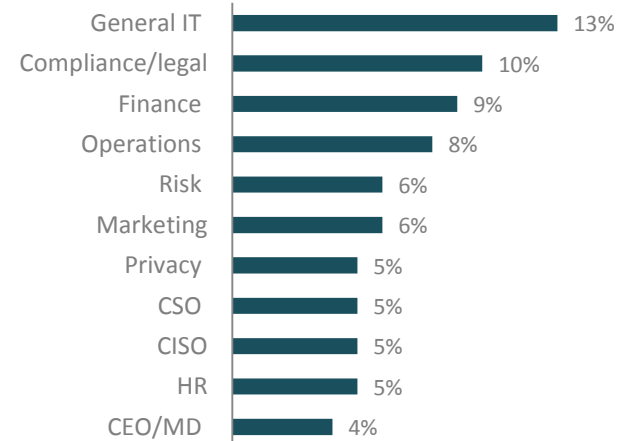
Survey: Industries and executive functions

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

Industries



Executive functions



Which of the following best describes your company's primary business? What is your title? To whom do you report?

Interviews

To gain further insights into cybersecurity risks and best practices, we interviewed a range of cybersecurity experts, practitioners, and technologists.

This included senior executives from the financial, technology, consumer markets, healthcare, legal, and consulting sectors.



Jason Harrell
Executive
Director, DTCC



Ryan Fritts
CISO, ADT



Kevin Mitnick
Chief Hacking
Officer, KnowBe4



Michael Varshavski
VP Operations,
CyberCube



Patrick Moorhead
President, Moor
Insights



Vali Ali
Chief Technologist, HP



Lee Kirschbaum
SVP, Product
Marketing, Opus



Chintan Jain
VP Security Engineering,
Security Mantra



Ron Mehring
VP Technology and
Security, Texas Health



David Estlick
CISO, Starbucks



Brian Henesbaugh
Partner, Baker
McKenzie



Matthew Johnson
CISO, Willis Towers
Watson



Larry Lidz
Global CISO, CNA
Financial



Dov Goldman
VP Innovation, Opus



Scott Laliberte
Managing Director,
Protiviti



Joseph Gittens
Technical
Standards, SIA



Mike Angle
CTO, Opus



Chintan Parekh
VP Cybersecurity,
Fidelity

Project team

To manage this pioneering research project, we brought together a multidisciplinary team from both ESI ThoughtLab and WSJ Pro Cybersecurity.

Louis Celi, Project Director, CEO, ESI ThoughtLab

Will Wilkinson, Publisher, WSJ Pro Cybersecurity

Dr. Daniel Miles, Chief Economist, ESI ThoughtLab

Julien Beresford, Survey Director, ESI ThoughtLab

Rob Sloan, Research Director, WSJ Pro Cybersecurity

Janet Lewis, Executive Editor, ESI ThoughtLab

Caroline Lindholm, Project Coordinator, ESI ThoughtLab

Laura Burtner, Graphic Designer, ESI ThoughtLab

Mike Daly, Marketing Manager, ESI ThoughtLab



Advisory board

To give us the benefit of their experience and insights into cybersecurity issues, we assembled a distinguished panel of executives.

| | | |
|---------------------------|---------------------------------------|-------------------------------|
| Brian Henesbaugh | Partner | Baker McKenzie |
| Michael Varshavski | Vice President of Operations | CyberCube |
| Jason Harrell | Cybersecurity Partnerships | DTCC |
| Robert Bussey | Cyber Threat Analyst | Evolver |
| Chintan Parekh | Business Info Security Officer | Fidelity |
| Boris Balacheff | VP and Chief Technologist | HP Inc. |
| Douglas Hubbard | Founder and Author | Hubbard Decision Research |
| Perry Carpenter | Chief Evangelist | KnowBe4 |
| Matthew Barrett | Cyber Framework Lead | NIST |
| Dov Goldman | Vice President, Innovation | Opus |
| Scott Laliberte | Managing Director | |
| Andrew Retrum | Managing Director | |
| Thomas Lemon | Managing Director | Protiviti |
| David Stanton | Managing Director | |
| Vince Dasta | Associate Director | |
| Don Erickson | Chief Executive Officer | Security Industry Association |
| Chintan Jain | VP Security Engineering | Security Mantra |
| Adeola Adele | Senior Director, Cyber Risk Solutions | Willis Towers Watson |

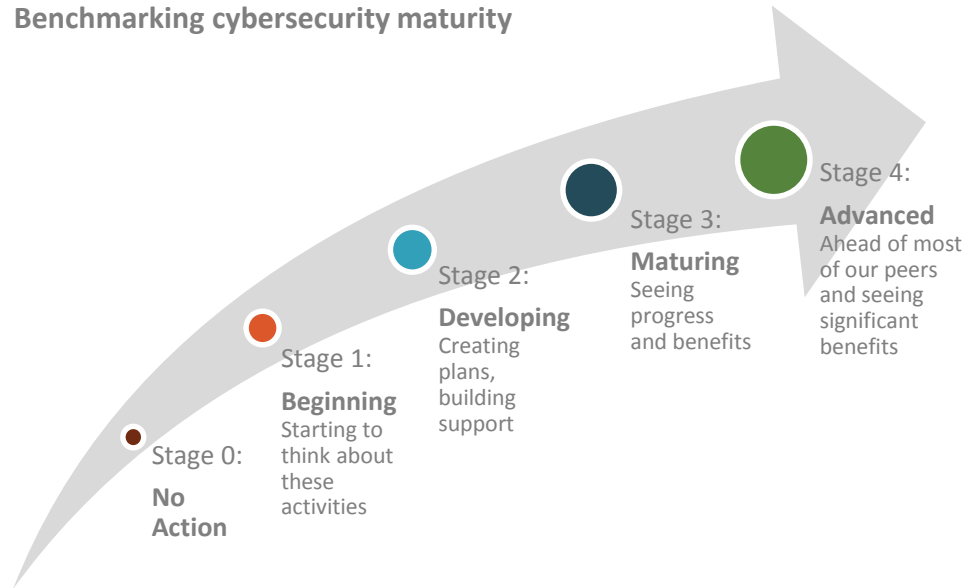
Microeconomic modeling

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

Respondents rated their progress against key activities under each category. For example, under the “detect” category, executives identified their progress with continuous security monitoring, testing detection processes, predictive analytics, and anomalies and impacts.

Our economists calculated category scores based on a ranking of 0 to 4 for each underlying activity. We summed the scores for each category to determine a composite score for each company for each category.

Benchmarking cybersecurity maturity



Respondents rated themselves on many components of cybersecurity using a five-point scale. We used their scores to sort them into three stages of cybersecurity maturity: beginners, intermediates and leaders.

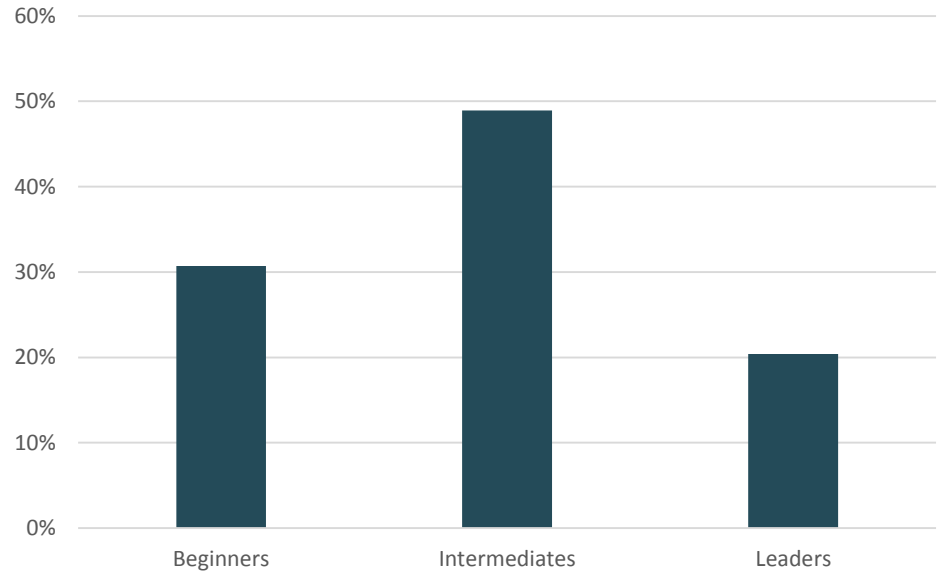
Defining cybersecurity maturity

To arrive at the maturity classifications, we first normalized the score range for each of the NIST categories. This was necessary because each of the categories had different numbers of sub-questions and thus a different maximum score.

We then took the geometric mean of each respondent's normalized scores across categories to arrive at an overall score. We classified respondents with a score less than the 30th percentile as beginners and those with a score greater than the 80th percentile as leaders. We classified the remainder as intermediates.

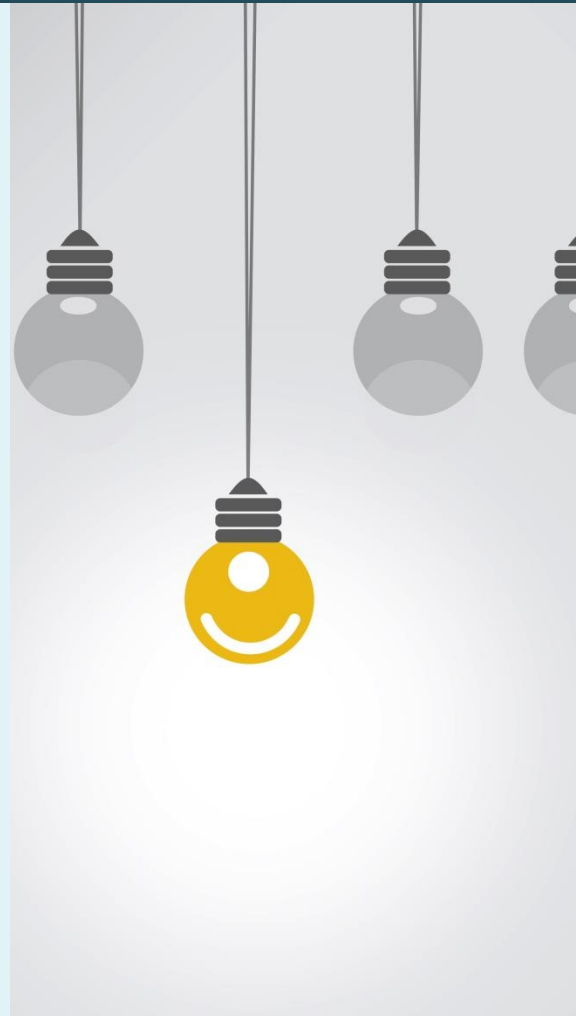
We applied an additional filter to the leaders to ensure that we only cited the best of the best. If two of a respondent's scores for individual categories were below average, we downgraded that company from a leader to an intermediate.

Benchmarking cybersecurity maturity



Acknowledgments

We would like to thank our sponsors and research partners for supporting this ground-breaking thought leadership program. They graciously provided valuable direction and research input throughout the course of the study. Without them, this program would not have been possible.

[Introduction](#)[Executive Summary](#)[Evolving Risk Landscape](#)[Road to Excellence](#)[Organizing for Cybersecurity](#)[Managing Cyber Risks](#)[Economics of Cybersecurity](#)[Measuring Cyber Risks](#)[Calls to Action](#)[Research Background](#)[Acknowledgements](#)

Special thanks to our sponsors

We would like to thank our sponsors and research partners for supporting this ground-breaking thought leadership program. They graciously provided valuable direction and research input throughout the course of the study. Without them, this program would not have been possible.



[Baker McKenzie](#) helps clients overcome the challenges of competing in the global economy. We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and fiends to instill confidence in our clients.



[CyberCube](#) delivers data-driven cyber analytics built specifically for the insurance industry. CyberCube is focused on solving the most difficult and important cyber risk challenges in insurance with world-class analytics. Our team is composed of multi-disciplinary experts across data science, cyber security, software engineering, actuarial modeling and commercial insurance.



[HP Inc.](#) creates technology that makes life better for everyone, everywhere. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we engineer experiences that amaze.



[KnowBe4](#) is the world's largest security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering. The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy security leaders and IT pros that have 16 other fires to put out. Our goal was to design the most powerful, cost-effective and easy-to-use platform.

Special thanks to our sponsors



[Opus](#) is a global risk and compliance SaaS and data solution provider founded on a simple premise: that faster, better decisions in compliance and risk management give businesses an extraordinary advantage in the marketplace. Today, the world's most respected global corporations rely on Opus to free their business from the complexity and uncertainty of managing customer, supplier, and third-party risks.



[Protiviti](#) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through its network of more than 80 offices in over 20 countries, Protiviti and its independently owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI).



[Security Industry Association \(SIA\)](#) is the leading trade association for global security solution providers, with more than 850 innovative member companies representing thousands of security leaders and experts who shape the future of the security industry. SIA protects and advances its members' interests by advocating pro-industry policies and legislation at the federal and state levels, creating open industry standards that enable integration, advancing industry professionalism through education and training, opening global market opportunities and collaborating with other like-minded organizations.



[Willis Towers Watson](#) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has over 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals.

Additional resources

[Bakermckenzie.com/-/media/minisites/tmt/files/2018/08/gdpr_national_legislation_survey_4_aug2018.pdf](https://www.bakermckenzie.com/-/media/minisites/tmt/files/2018/08/gdpr_national_legislation_survey_4_aug2018.pdf)

[Globaltmt.bakermckenzie.com/data-protection-enforcement](https://globaltmt.bakermckenzie.com/data-protection-enforcement)

[Globaltmt.bakermckenzie.com/data-security](https://globaltmt.bakermckenzie.com/data-security)

[Globaltmt.bakermckenzie.com/global-privacy-matrix](https://globaltmt.bakermckenzie.com/global-privacy-matrix)

[Knowbe4.com/resources](https://www.knowbe4.com/resources)

[Protiviti.com/Cybersecurity](https://www.protiviti.com/Cybersecurity)

[Protiviti.com/Cybersecurity-FS](https://www.protiviti.com/Cybersecurity-FS)

[Protiviti.com/FAIR](https://www.protiviti.com/FAIR)

[Protiviti.com/GDPR](https://www.protiviti.com/GDPR)

[Protiviti.com/ThreatReport](https://www.protiviti.com/ThreatReport)

[Securityindustry.org/report/sia-cybersecurity-advisory-board-enterprise-security-recommendations/](https://www.securityindustry.org/report/sia-cybersecurity-advisory-board-enterprise-security-recommendations/)

[Willistowerswatson.com/cyber](https://www.willistowerswatson.com/cyber)

The Cybersecurity Imperative

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

Lou Celi, Project Director

917.459.4616 | Lceli@esithoughtlab.com

Barry Rutizer, Client Director

917.251.4190 | Brutizer@esithoughtlab.com

Dr. Daniel Miles, Chief Economist

215.717.2777 | Miles@econsultsolutions.com

Caroline Lindholm, Project Coordinator

215.717.2777 | Lindholm@econsultsolutions.com

About ESI ThoughtLab

ESI ThoughtLab is an innovative thought leadership and economic research firm providing fresh ideas and evidence-based analysis to help business and government leaders cope with transformative change. We specialize in analyzing the impact of technological, economic, and demographic shifts on industries, cities, and companies. ESI ThoughtLab is the thought leadership arm of Econsult Solutions, a leading economic consultancy with links to the academic community.

About WSJ Pro Cybersecurity

A division of the Wall Street Journal, WSJ Pro Cybersecurity is designed to help executives monitor the ever-changing landscape of cybersecurity through a business lens. Our dedicated team delivers unique, actionable insight on the wide-ranging challenges of cybercrime risk.

Visit: www.esithoughtlab.com

