WSJ PRO CYBERSECURITY

ESI THOUGHTLAB

THE CYBERSECURITY IMPERATIVE

PROJECT SPONSORS

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

Introduction

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

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

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

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

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

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

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

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

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

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

If an organization aims to *effectively manage* cyber risk, continuous investment and improvement are critical and support from senior executives is required.

Key Findings

This is a first-of-its-kind study and produced a wealth of valuable data about how companies across multiple geographies and industries are approaching cybersecurity. Here are a few of the key findings:

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

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

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

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

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

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

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

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

NIST Cybersecurity Maturity

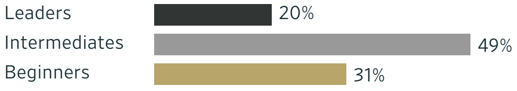
One of the hardest problems many businesses, particularly small businesses, have with cybersecurity, is where to start. The number of potential starting points can be overwhelming, which is why the National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework. The framework is business-focused and guides organizations in their management of cyber risk and communication of the risks to senior management and the board.

Based on our survey findings and a custom scoring model developed by ESI Thoughtlab, just under half of companies (49%) are in the intermediate stage of cybersecurity maturity, while 31% are beginners and only 20% are leaders. This clearly demonstrates there is considerably more that firms should do to secure their business and customer information from cyberattacks.

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 billion 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 for them to do more damage—these safeguards will not completely prevent hackers from breaking in. Companies would be wise to focus more on response and recovery.

Figure 1. Organizations by Cybersecurity Maturity



% of firms by cybersecurity stage

In terms of where companies are performing well against NIST categories, good progress is being made on access control and analysis of incidents (39% of companies are doing both of these), network monitoring to detect security events (36%), creating written policies and procedures (35%) and managing data in line with the risk management strategy (34%).

An overwhelming 87% of survey respondents pointed to untrained general staff as a top risk due to the continued high frequency of cybercriminals sending phishing attacks as a way of compromising corporate networks. Despite this, staff training is towards the bottom of a list of NIST categories that companies have addressed.

The categories most companies appear to be struggling with include detecting anomalous activity (only 13% of companies are performing well against this category), understanding policies and processes related to the management of risk and requirements (11%) and the ability to contain the spread of security incidents to prevent further harm (11%).

Figure 2. Progress Against NIST Categories

Top Seven NIST Categories		NIST Function	Bottom Seven NIST Categories		NIST Function
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

Figure 3. Cybersecurity Maturity by Industry

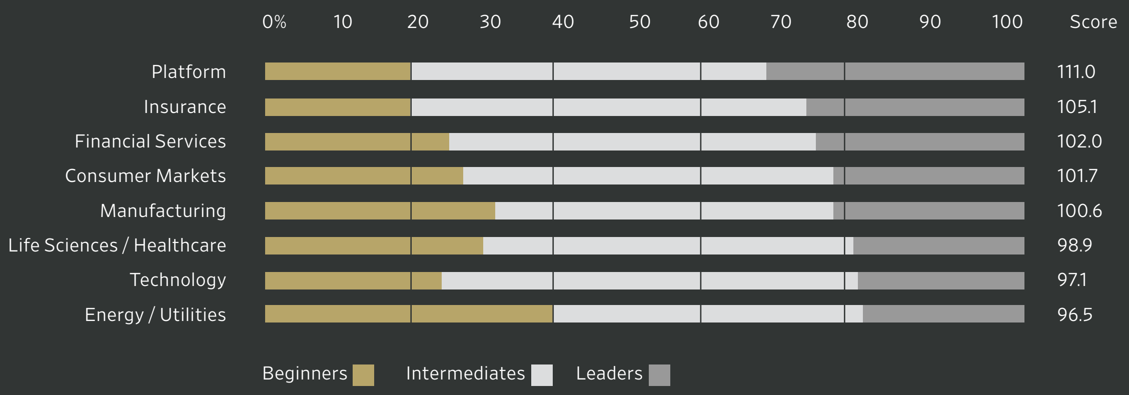
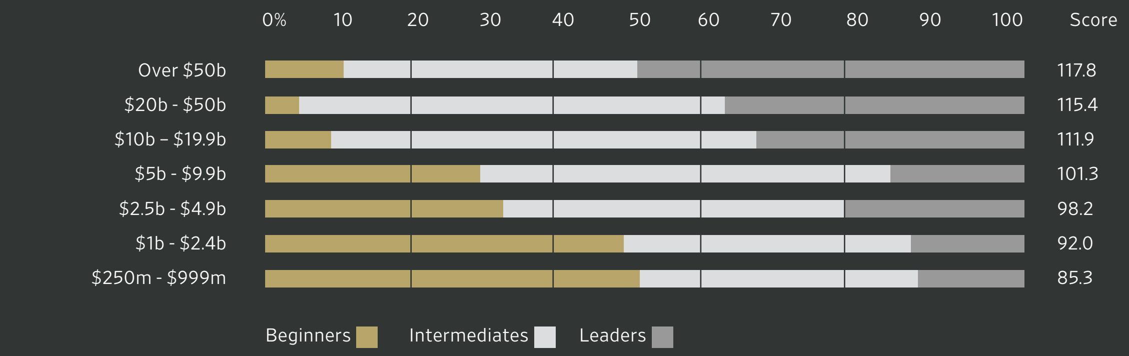


Figure 4. Cybersecurity Maturity by Revenue

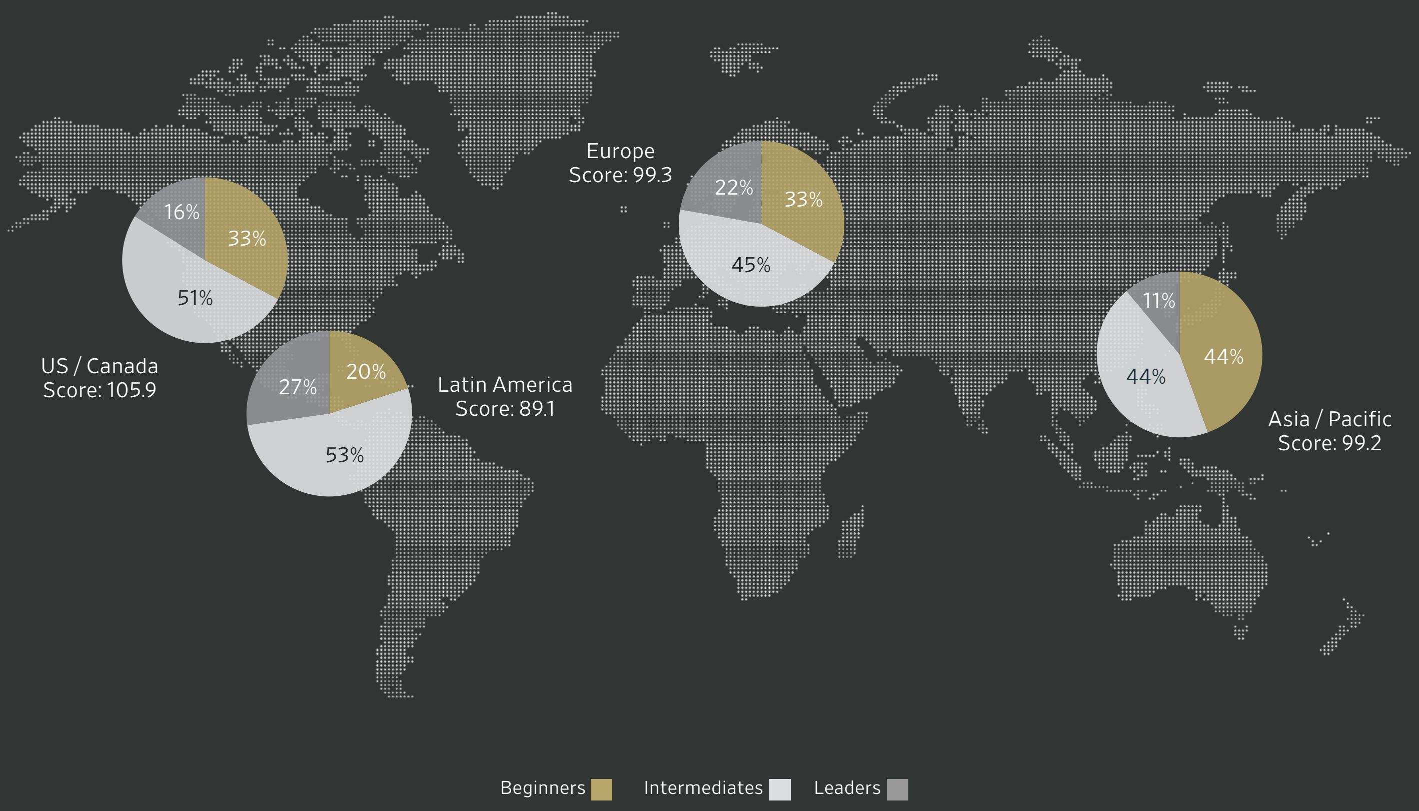


To facilitate benchmarking, we developed cybersecurity maturity scores based on the progress against the five categories of the NIST Cybersecurity Framework, with 100 as the average.

Born-digital 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.

Our data shows a correlation between company size and cybersecurity maturity. Companies with revenues over $50 billion have the highest cybersecurity scores while firms with sales below $1 billion have the lowest. This suggests small businesses have a lot of work to do.

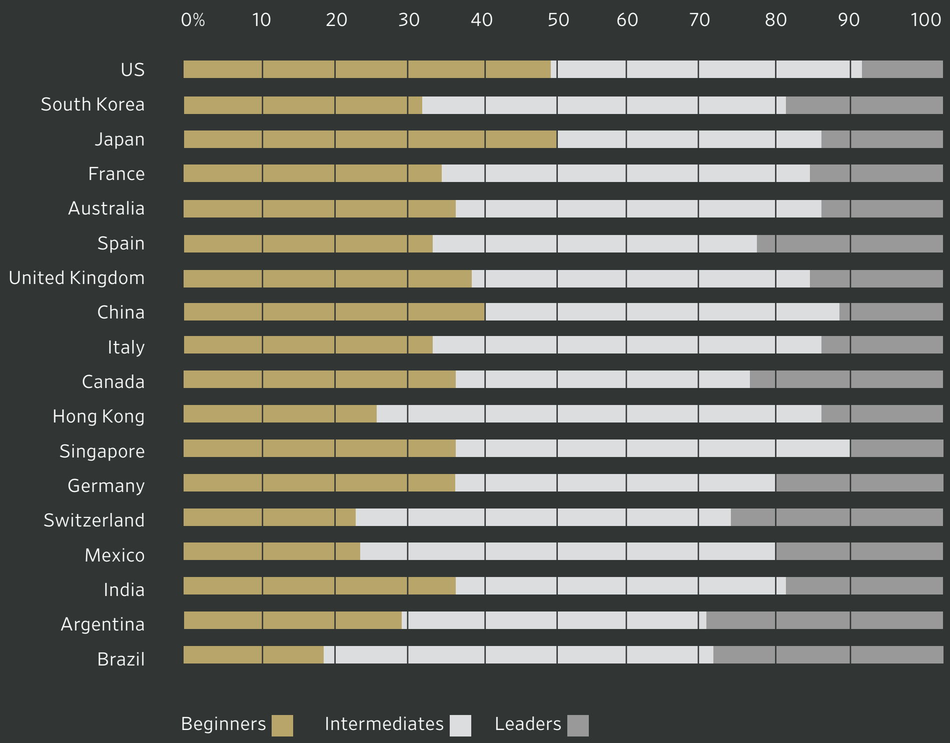
Figure 5. Cybersecurity Maturity by Region



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.

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

Figure 6. Cybersecurity Maturity by Country



Digital maturity often goes hand-in-hand with cybersecurity maturity. According to the data, 68% of digital beginners are also cybersecurity beginners. Just 3% of those companies that are digital beginners are cybersecurity leaders. The correlation holds true for leaders too. Almost half (46%) of digital leaders are also cybersecurity leaders, while only 6% of digital leaders are cybersecurity beginners.

Nonetheless, a disconcertingly large proportion of digital leaders (over half) are not cybersecurity leaders and this leaves them exposed to cyber risk that could seriously disrupt the technologies these businesses rely so heavily upon.

Overall, the results of our study suggest growth and progress in cybersecurity maturity are not keeping pace with digital transformation efforts underway in most companies. All organizations on a journey of digital transformation should be mindful of the connection between new technology and increased cyber risk. A balance must be found between the two in order to manage that risk. Security must be an integral part of efforts to digitize processes and certainly not act as a blocker. Risks will increase as organizations make more of their services and data accessible online, often globally, and start to rely more on technologies such as mobile applications, cloud platforms, Internet of Things, APIs, and blockchain.

The Economics of Cybersecurity

Cybersecurity does not come cheap. Salaries for skilled cybersecurity staff are high, as is the cost of third-party consultancy expertise. Technical solutions and assurance work are essential, but can also put large holes in the cybersecurity budget. However, these costs pale in significance compared to the costs associated with remediating a data loss or other major security event.

There is no such thing as security, only degrees of insecurity. No amount of investment will ever guarantee an organization's security, however, continued investment in people, process and technologies is vital if organizations are to build effective defenses that keep attackers out and minimize their ability to do damage if they do breach network defenses.

Our survey asked a number of questions related to the way organizations spend money on cybersecurity —how much they spend, the amount they spend as a proportion of their information technology budget, and how they spend it. Analyzing cybersecurity spending over a three-year period shows a clear pattern: The percentage of budget allocated to identification and detection decline, and the amount apportioned to protection, response, and recovery rise.

Protection spending is higher than any other activity. Our research shows that with regards to cybersecurity, protection will continue to be the main focal point for investment across all industries next year, with insurance companies spending the most—29% of their cybersecurity budget—and financial services the least at 25%.

Protection activities are typically expensive (such as, but not limited to) assurance testing and security software solutions, but it is also true that no CISO wants to have underinvested in products or services that could save the company from a major breach. In the longer term, CISOs must ensure they are balancing their investments to avoid neglecting any one activity.

As companies begin applying their cybersecurity frameworks, they tend to invest mostly in protection, detection, and identification, and spend less on response and recovery. However, as companies become more advanced in cybersecurity, they increase their investment in response and recovery. For example, cybersecurity beginners spend 14% on recovery, while leaders spend 18%.

While spending on technology tapers as firms mature, it still accounts for the largest slice of their cybersecurity budgets.

Figure 7. Cybersecurity Spending by Maturity and NIST Category

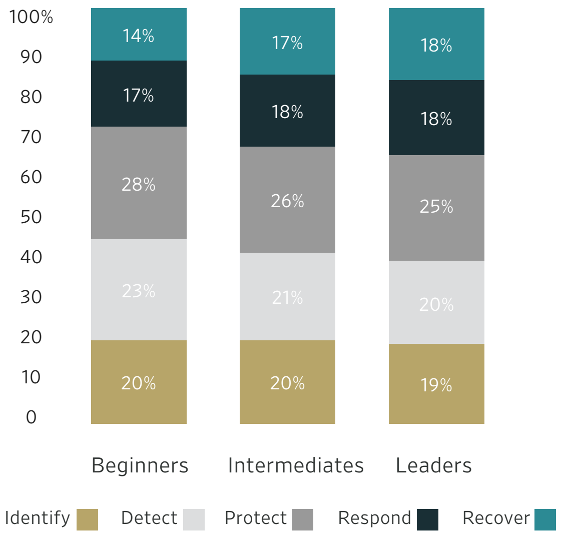


Figure. 8 Cybersecurity Spending by Year and NIST Category

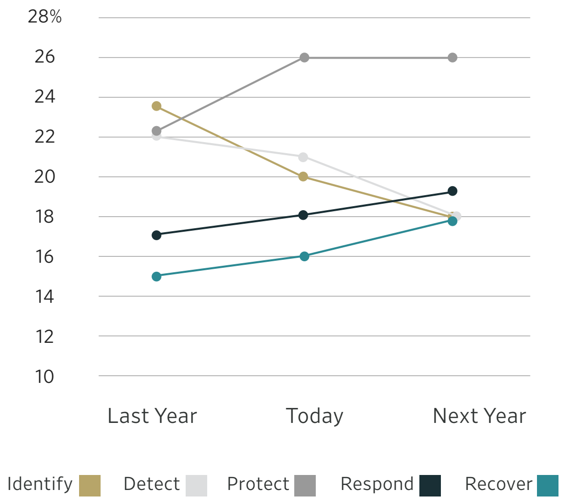
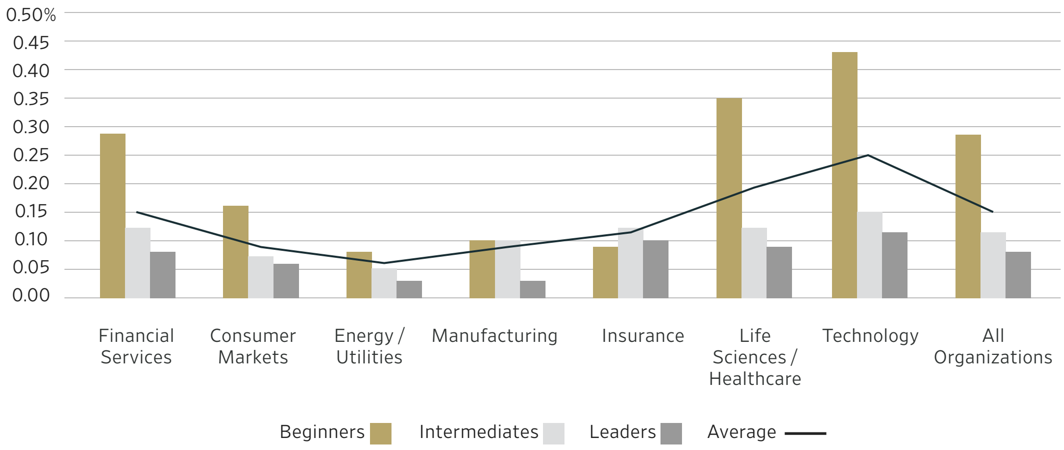


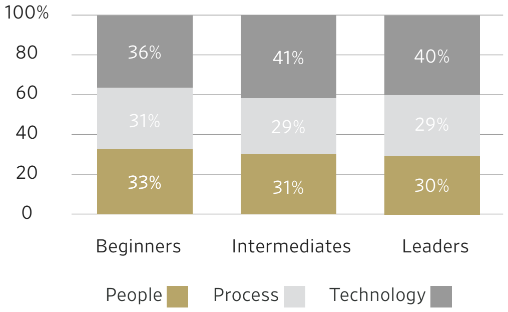
Figure 9. Cybersecurity Spending as a Percentage of Revenue



Investing wisely in people, process, and technology is crucial for cybersecurity success. Investment in people and process declines as cybersecurity maturity advances, while technology spending grows.

Experts say that although training can have a lot of impact—before training, 28% of employees will click on a phishing link, while after, only 2% will—there are limits to its effectiveness. Without technology backstops, one employee clicking on a malware link can create havoc. However, the lack of investment in automating processes could be a mistake. When security technologies can be orchestrated to talk to one another, and perhaps even take action on routine scenarios, security personnel can focus on other tasks that really require human skills. Automation can therefore help compensate for the shortage of cybersecurity talent.

Figure 10. Investment in People, Process and Technology by Cybersecurity Maturity

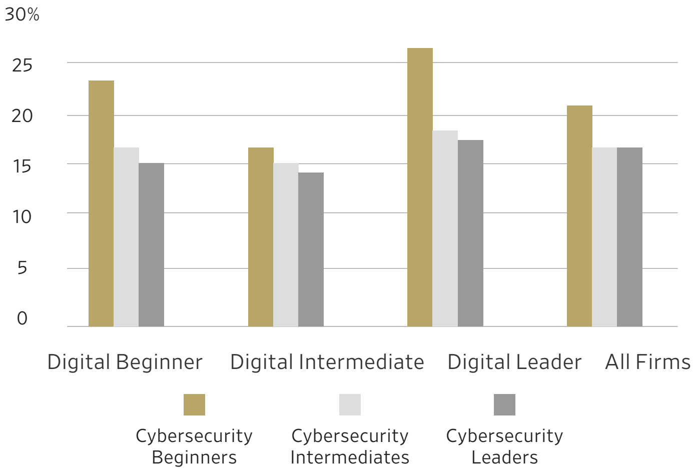


Across all firms, cybersecurity beginners have a higher probability of suffering a successful cyberattack that results in more than $1 million in losses—about 21%, while that for cybersecurity leaders the average is 16%.

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, the likelihood rises to 27%.

Figure 11. Probability of Having More than $1 Million in Losses



While firms believe that the probability of a successful attack decreases as they move up the cybersecurity maturity curve, our analysis shows a different story. Firms just starting their cybersecurity journey, regardless of sector, report fewer successful attacks per year than companies that are further along the cybersecurity maturity curve. Beginners also report fewer customer records lost or stolen than more mature companies do.

One reason for the seemingly anomalous results—a higher rate of successful attacks on more cybersecurity-mature companies—is that cybersecurity leaders are generally more advanced in digital transformation. This exposes them to greater risks, particularly if digital transformation outpaces their cybersecurity measures.

However, perhaps the most likely explanation is that cybersecurity beginners have substandard detection measures and thus may be under-reporting their numbers on 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 hacked.

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

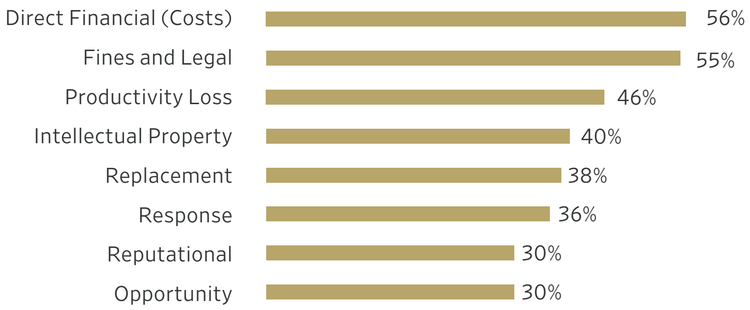
Firms are more likely to measure the costs that involve actual dollars, such as the direct financial costs, replacement costs or fines and legal costs. Nearly all survey respondents measure these costs.

On the other hand, 11% of firms 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.

Cybersecurity beginners see a larger cost from cyber attacks than companies further along the curve—just under .04% (about $4 million for a company with $10 billion in revenue), while costs average just over .01% of revenue for more cyber-mature companies.

There are large differences across industries: life science and technology companies report higher costs—around .05% of revenue for beginners—than energy and insurance firms.

Figure 12. Percentage of Businesses Impacted by Post-Breach Cost Types



How Organizations Perceive Threats and Risks

Two of the key drivers of the cybersecurity market are threat and risk. These factors are constantly changing as threat actors evolve and technological change brings new risks. The perception of threat and risk will, in many cases, determine how seriously an organization takes cybersecurity and how much it invests in taking steps to reduce risk.

Perceptions of threat will be based on various factors including, but not limited to, the organization's previous experience of attacks and their impact, the experiences of peer organizations, the value ascribed to company data, advice provided by expert third parties or government agencies and the leadership team's own personal knowledge of threat actors and their motivations. This combination will be unique to all businesses.

In terms of risk, the perception will also be driven by a number of discrete factors such as the digital maturity of the business, the identification of existing risks and confidence in how well they have been addressed, the implementation rate of new or untested technology and the dependence of the business on technologies or software known to have regular security issues.

We asked 1,300 organizations at a high level about the threat actors that concern them the most and the results were somewhat surprising.

The group identified as the greatest threat were unsophisticated hackers with 59%, slightly ahead of cybercriminals with 57%. These two groups do have some significant overlap of course—many unsophisticated hackers will be motivated by financial gain and many cybercriminals are anything but sophisticated. It is certainly true that there are far more unsophisticated hackers sending out potentially damaging attacks on a massive scale than there are high-end criminals doing the same thing.

Only 3% of respondents identified government-sponsored hackers as a key threat for their business. While this figure may seem low, the fact is that nation-states are not attacking the private sector on a massive scale. Attacks are targeted carefully and only those businesses that hold data of value to a state are likely to be impacted. Of course, nation-states do steal intellectual property that has a commercial value, but very few businesses hold this data.

Interestingly, 'hacktivists', the name given to individuals motivated to attack an organization in the name of a cause, represent a threat to just over four in ten businesses. The perceived threat of hacktivism is in contrast to the reality of hacktivism. In the last five years the number of attacks fueled by hacktivist groups such as Anonymous has fallen dramatically following successful law enforcement actions.

Almost a third (29%) identified malicious insiders as a cybersecurity threat. Though malicious insiders undoubtedly cause damage and are a source of data loss for companies, the majority of insiders exploit their legitimate access to systems and data rather than gaining unauthorized access through security bypasses.

In each case, cybersecurity leaders were more concerned about threat actors than those deemed to be cybersecurity beginners.

Three other groups of internal staff were identified as cybersecurity risks: 20% of those surveyed stated contractors represented a significant risk, 29% highlighted privileged users (those users with administrator level access, usually working in the I.T. department) and an overwhelming 87% of respondents viewed untrained staff as a cybersecurity risk. Attackers understand this, which is why email phishing attacks, especially those targeted at individuals, are so successful. It is however easy to forget that if a user infects the network by interacting with a phishing email, every other technical defense the organization invested in has failed.

Figure 13. Perception of Threat by Threat Actor and Cybersecurity Maturity

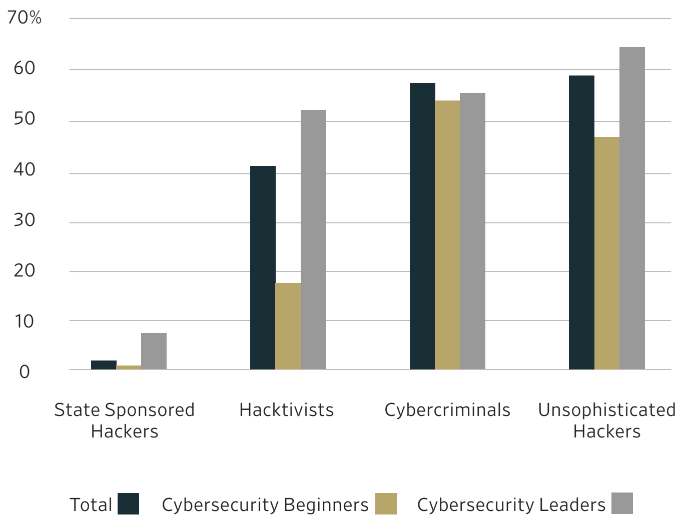
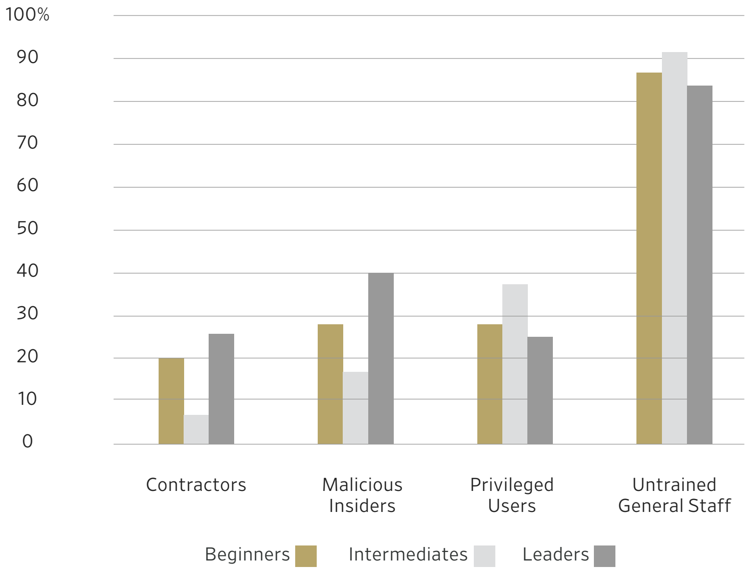


Figure 14. Perception of Risk by Internal Staff Role and Cybersecurity Maturity



Surveyed organizations were asked about the types of attacks they see and 81% reported that malware and spyware were having an impact on their business. Perhaps surprisingly, the degree of impact varied widely, with 64% of organizations headquartered in the US & Canada reporting an impact, but 96% of the organizations in Asia Pacific reporting an impact.

For ransomware attacks the picture was even starker: 63% saw an impact overall, but only 48% in the US and Canada compared to 82% in Asia Pacific.

Companies in Latin America see a greater number of attacks through the supply chain than other regions—57% compared to the global average of 32%.

Organizations were also asked about how they think attacks will impact them in two years' time; the responses were far from positive. Respondents predicted every single threat category was more likely to impact their company in two years with 82% of organizations ranking attacks through mobile applications as their greatest concern. Denial of service attacks are currently a concern for 29% of people, but 70% see denial of service as something that will impact their organization in two years' time.

Asia Pacific typically viewed future threats more negatively, but one increase in particular stood out: while just 8.8% of companies in Asia Pacific state attacks on their partners, customers, vendors and intermediaries are having an effect on their business now, 83.3% said the same attacks will have an effect in two years—an increase of around 850%.

The increasing complexity of networks and their interconnectivity—'ecosystem growth'—is seen as a key risk due to larger and more complex relationships to manage, increased data sharing with suppliers and partners and more integrated supply chains.

Figure 15. Perception of Risk Now and in Two Years

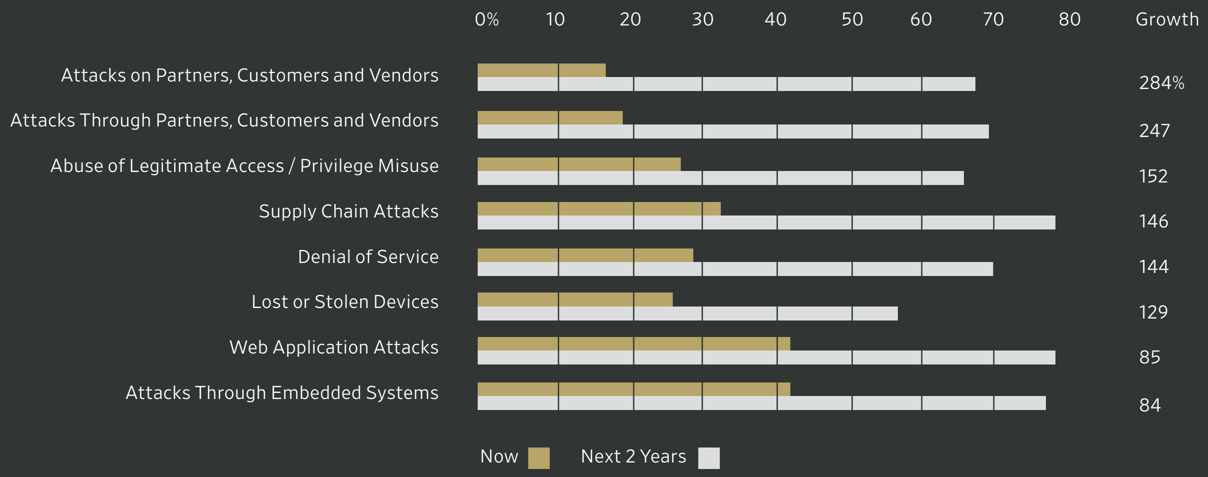
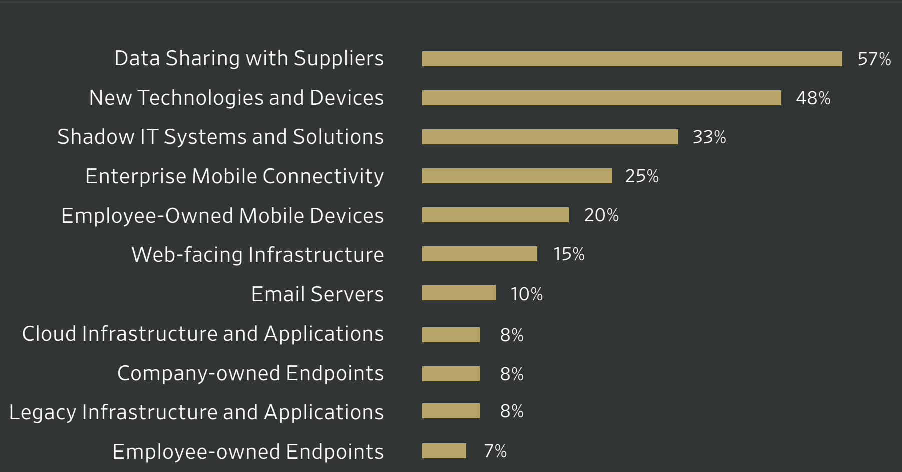


Figure 16. Greatest Risks Identified by All Organizations



Governance and Strategy

Cybersecurity can be a serious challenge for all involved. Cybersecurity governance is complicated by the fact the discipline is still reasonably new as a business-critical function. Different industries attach different degrees of priority to cybersecurity that can affect reporting lines and ultimate corporate responsibility.

The Chief Information Security Officer is the role most favored (27%) as being responsible for cybersecurity. Various other C-suite positions were also reported as being 'owners' of cybersecurity including, unsurprisingly, the CIO or CTO (19%) and, perhaps more surprisingly, the Chief Privacy Officer or Chief Data Protection Officer (15%).

Chief Privacy Officers or Chief Data Protection Officers are more likely to have responsibility for cybersecurity in Europe or the US & Canada (around 20% of organizations) or in life sciences and consumer markets companies—17% and 18% respectively.

One reason for the rise in privacy and data protection officers is undoubtedly the regulatory environment. The introduction of the General Data Protection Regulation (GDPR) earlier this year affecting any company holding data on European Union citizens, regardless of where the company is actually based, and the draconian penalties for those in breach of the regulation will have focused the minds of board members. Whether this trend continues depends largely on which new regulations will emerge and to what extent cybersecurity becomes compliance-focused.

Figure 17. Executive Responsibility for Cybersecurity

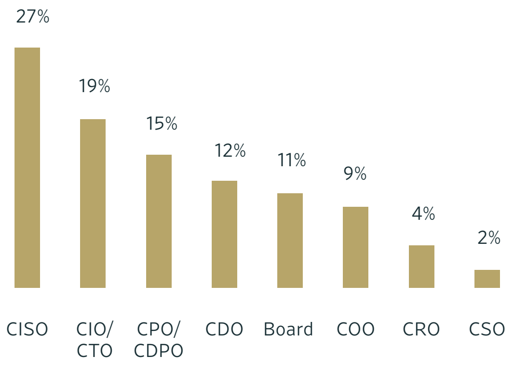
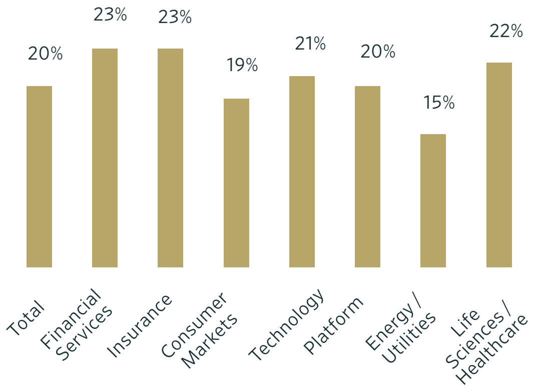


Figure 18. Percentage of Organizations with a Data Protection Officer



Calls to Action

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

1. Getting The Basics Right

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

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

For instance:

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

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

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

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

Cybersecurity hygiene is only part of the solution. It does not prevent attacks or guarantee protection, but *it reduces risk* and is effective at reducing the number of incidents internal resources must attend to, allowing more time to dedicate to more significant issues.

2. Ongoing Cybersecurity Awareness

Our survey found an overwhelming majority of respondents viewed untrained employees as the greatest cyber risk to their businesses. This is not to say that users, untrained or otherwise, are stupid, negligent, careless or reckless, it is simply to say that criminals and attackers use this vector of attack the most. Attackers socially engineer victims to click on links or to open attachments that will result in their machines becoming infected. Sophisticated attackers meticulously research their victims in order to create the most authentic looking emails, which their victims will most likely interact with.

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

According to a recent survey[1], only 5% of organizations run a mature cybersecurity awareness program. Programs take time to build, must be supported by senior executives and have full-time resource allocated to them. Communications skills should be valued over security skills–employees will only learn if the content is engaging and relevant. Finally, the training must be ongoing and tailored to individual needs with regular updates if a change in culture is to be achieved.

Many organizations choose to conduct phishing attacks against their staff to better understand how effective cybersecurity awareness training has been for staff and to identify individual employees that may be more susceptible to phishing in order to target remedial training.

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

[1] See pge 30 of 2018-SANS-Security-Awareness-Report

In an age when applications are being created and *updated more frequently* than ever before, it is essential that security is an integral part of the development process.

3. Baking Security In, Not Bolting Security On

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

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

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

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

Lack of preparation leaves companies *dangerously exposed* to severe operational impact in the case of a cybersecurity incident.

4. Resilience Through Exercises

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

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

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

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

At the senior level, the discussions and the plans that need to be put in place are different. Bringing senior decision-makers together to get familiar with the types of incident that could affect the company is paramount to understanding the risks they bring. A CEO must confide not only that the technical response is adequate, but also that the company will have access to the best legal and communications expertise to help manage fallout from the incident and sufficient insurance to cover post-breach expense–for example, the costs associated with notifying customers of a breach.

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

Cyber is simply one more *business risk*, albeit with significant consequences if it is not managed effectively.

5. Board-Level Engagement

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

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

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

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

Money wasted on the wrong service or product, or money spent mitigating the wrong risks could result in *security breaches* that cost the organization dearly.

6. Investment with Impact

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

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

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

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

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

Our respondents included *organizations in all major world regions,* from those with under $1 billion in revenue to very large enterprises with over $50 billion.

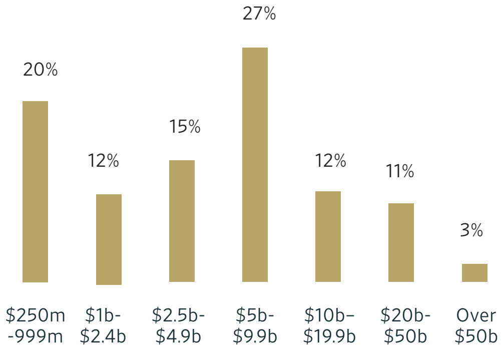
Research Background

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

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

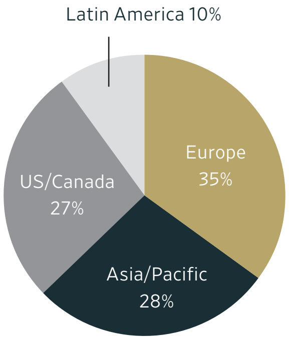
Our survey respondents included executives from organizations in all major world regions, spanning companies with under $1 billion in revenue to very large enterprises with over $50 billion in revenue. To ensure the breadth of our analysis, we also included public companies (70% of total), private companies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

Figure 19. Responses by Company Revenue



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

Figure 20. Survey Response by Region



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

Figure. 21 Survey Responses by Industry

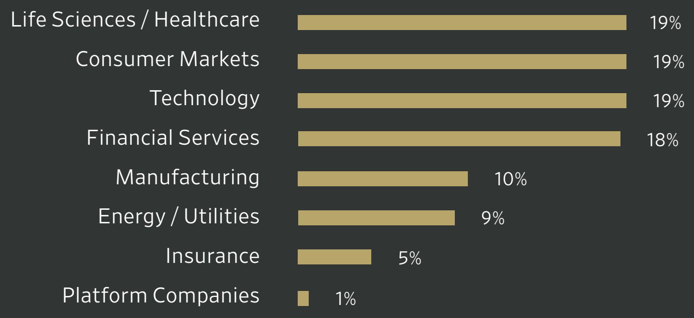
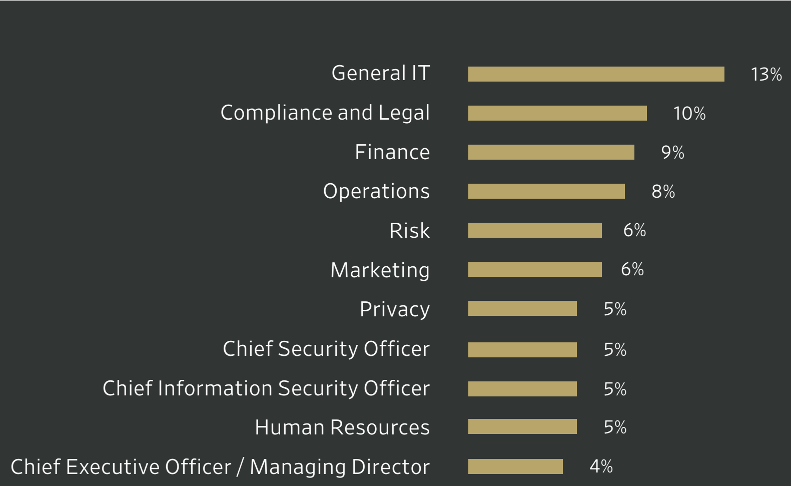


Figure. 22 Survey Responses by Executive Role



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

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

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

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. We then aggregated the scores to show trends by industry, location, revenue, size and other key parameters. We used these scores to segment respondents into maturity stages and to benchmark their performance.

To gain further insights into cybersecurity risks and best practices, we interviewed a range of cybersecurity experts, practitioners, and technologists. These included senior executives from the financial, technology, consumer markets, healthcare, legal, and consulting sectors.

Research Partners

ESI THOUGHTLAB

CyberCube

Baker McKenzie.

hp

KnowBe4
Human error. Conquered.

protiviti®
Face the Future with Confidence

Willis Towers Watson

opus

SIA
SECURITY INDUSTRY ASSOCIATION