Is cybersecurity about more than protection?

EY Global Information Security Survey 2018-19

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

Welcome

Paul van Kessel

EY Global Advisory Cybersecurity Leader

Welcome to the 21st *EY Global Information Security Survey* (GISS) exploring the most important cybersecurity issues facing organizations today.

More than two decades after EY began researching organizations' awareness of the growing cybersecurity threat — and their response — the need to engage with this issue from board level down is more pressing than ever. Attacks continue to grow in both number and sophistication. The range of bad actors is expanding. And digital transformation and new technologies are exposing organizations to new vulnerabilities.

This year, we are delighted that more than 1,400 respondents have taken the time to participate in our research — we are grateful to all of you. EY analysis of the responses from CIOs, CISOs and other executives shows that many organizations are increasing the resources they devote to cybersecurity, but also that they remain deeply concerned about the scale and severity of the threat.

That is as it should be. Cyber risks are evolving; any organization that regards itself as safe from cyber attack is likely to be in for a shock.

Moreover, the objective for all organizations should be to not only protect the enterprise with good cybersecurity hygiene and basic lines of defense, but also to optimize the response with more advanced tools and strategies. As digital transformation proceeds, cybersecurity must be an enabling function rather than a block to innovation and change.

This year's GISS explores these themes in more detail. By sharing ideas and leading practices, we can improve cybersecurity for all.

Contents

01 The future state of cybersecurity

After a year in which organizations have been rocked by a series of large-scale cybersecurity breaches and ongoing recriminations over state-sponsored interventions, this year's *EY Global Information Security Survey* (GISS) shows cybersecurity continuing to rise up the board agenda. Organizations are spending more on cybersecurity, devoting increasing resources to improving their defenses, and working harder to embed security-by-design.

However, the survey results also suggest that organizations need to do more. More than three-quarters (87%) of organizations do not yet have a sufficient budget to provide the levels of cybersecurity and resilience they want. Protections are patchy, relatively few organizations are prioritizing advanced capabilities, and cybersecurity too often remains siloed or isolated.

The challenge is for organizations to progress on three fronts:

- **Protect the enterprise**. Focus on identifying assets and building lines of defense.
- **Optimize cybersecurity**. Focus on stopping low-value activities, increasing efficiency, and reinvesting the funds in emerging and innovative technologies to enhance existing protection.
- **Enable growth**. Focus on implementing security-by-design as a key success factor for the digital transformations that most organizations are now going through.

These three imperatives must be pursued simultaneously. The frequency and scale of the security breaches all around the world show that too few organizations have implemented even basic security.

However, even as they seek to catch up, organizations must also move forward, fine-tuning existing defenses to optimize security and support their growth. As the digital transformation agenda forces organizations to embrace emerging technologies and new business models — often at pace — cybersecurity needs to be a key enabler of growth.

It's not easy … do you recognize this?

6.4 billion

The number of fake emails sent worldwide – every day[1]

1,464

The number of government officials in one state using "Password123" as their password[2]

50%

The number of local authorities in England relying on unsupported server software[3]

2 million

The number of stolen identities used to make fake comments during a US inquiry into net neutrality[4]

1,946,181,599

The total number of records containing personal and other sensitive data compromised between January 2017 and March 2018[5]

US$729,000

The amount lost by a businessman in a scam combining "catphishing" and "whaling"[6]

550 million

The number of phishing emails sent out by a single campaign during the first quarter of 2018[7]

US$3.62m

The average cost of a data breach last year[8]

[1] Dark Reading, August 27, 2018. [https://www.darkreading.com/endpoint/64-billion-fake-emails-sent-each-day/d/d-id/1332677]

[2] The Washington Post, August 22, 2018. [https://www.washingtonpost.com/technology/2018/08/22/western-australian-government-officials-used-password-their-password-cool-cool/]

[3] Computing, August 23, 2018. [https://www.computing.co.uk/ctg/news/3061558/fifty-per-cent-of-councils-in-england-rely-on-unsupported-server-software]

[4] Naked Security, 24 May 2018. [https://nakedsecurity.sophos.com/2018/05/24/2-million-stolen-identities-used-to-make-fake-net-neutrality-comments/]

[5] Chronology of Data Breaches, March 2018. [https://www.privacyrights.org/data-breaches]

[6] SC Media, 28 December 2017. [https://www.scmagazine.com/home/resources/email-security/australian-loses-1-million-in-catphish-whaling-scam/]

[7] Dark Reading, 26 April 2018. [https://www.google.co.uk/search?q=New+Phishing+Attack+Targets+550M+Email+Users+Worldwide&oq=New+Phishing+Attack+Targets+550M+Email+Users+Worldwide&aqs=chrome..69i57.363j0j4&sourceid=chrome&ie=UTF-8]

[8] Ponemon Institute, July 2017. [https://www.ponemon.org/blog/2017-cost-of-data-breach-study-united-states]

02 Protect the enterprise

Our analysis suggests that significant numbers (77%) of organizations are still operating with only limited cybersecurity and resilience. They may not even have a clear picture of what and where their most critical information and assets are — nor have adequate safeguards to protect these assets.

That is why it is important for most organizations to continue to zero in on the very basics of cybersecurity. They should first identify the key data and intellectual property (the "crown jewels"), then review the cybersecurity capabilities, access-management processes and other defenses, and finally upgrade the shield that protects the company.

Questions that organizations must consider:

- What are our most valuable information assets?
- Where are our most obvious cybersecurity weaknesses?
- What are the threats we are facing?
- Who are the potential threat actors?
- Have we already been breached or compromised?
- How does our protection compare with our competition?
- What are our regulatory responsibilities, and do we comply with them?

In this chapter, we look at the four vital components of protecting the enterprise:

1. **Governance.** Organizations should address the extent to which cybersecurity is an integral part of the strategy of the organization, and whether there is enough funding for the necessary investment in defense.
2. **What is at stake?** What do organizations fear most, and how do they regard the biggest threats they are facing?
3. **Protection.** The maturity of the cybersecurity of an organization and the most common vulnerabilities are key.
4. **Breaches.** How breaches are identified and the way in which organizations respond are critical issues.

One overarching problem is skills shortages: estimates identify a global shortfall of about 1.8 million security professionals within five years.[9] Even in the most well-resourced sectors, organizations are struggling to recruit the expertise they need.

Financial services is one example. "The evidence in financial services is increasingly that the best graduates no longer want to work in the industry, which is hampering efforts to recruit across the sector," says Jeremy Pizzala, EY Global Financial Services Cybersecurity Leader.

Attracting more women and minorities into the cybersecurity workforce — both to swell the numbers and to build a resource better able to counter the threat — is a challenge in itself. "The industry needs to spearhead concerted efforts to fill the ranks, and do so properly, with women and minorities," says Shelley Westman, a principal with Ernst & Young LLP cybersecurity team. "Diversity is a business imperative. Diverse teams drive better results across the organization. They are more innovative, objective and collaborative. That's critical in cybersecurity where every day is a fight to stay a step ahead of the attackers."

[9] EY Cybersecurity Summit, June 2018. [[https://www.ey.com/gl/en/issues/governance-and-reporting/center-for-board-matters/ey-understanding-the-cybersecurity-threat]]

1. Governance

Is cybersecurity part of the strategy? And is it in the budget ?

More than half of the organizations don't make the protection of the organization an integral part of their strategy and execution plans. Surprisingly, larger organizations are more likely to fall short on this point than smaller organizations (58% versus 54%).

The good news is that cybersecurity budgets are on the rise. However, larger companies are more likely to increase budgets this year (63%) and next (67%) than smaller companies (50% and 66%).

> As digital transformation agendas continue to dominate, a bigger cybersecurity budget is necessary. Almost all companies are looking at technologies such as robotics, machine learning, artificial intelligence, blockchain and so on. All of that change will come with additional cyber risks and necessary investments."
>
> **Mike Maddison,**
> EY EMEIA Cybersecurity Leader

How organizations' total cybersecurity budget is set to change in the next 12 months:

	This year	Next year
Increased by more than 25%	12%	15%
Increased between 15% and 25%	16%	22%
Increased between 5% and 15%	25%	28%
Stayed approximately the same (between +5% and -5%)	40%	31%
Decreased between 5% and 15%	4%	2%
Decreased between 15% and 25%	1%	1%
Decreased by more than 25%	1%	1%

39% Say that less than 2% of their total IT headcount work solely in cybersecurity

55% Of organizations do not make 'protecting' part of their strategy

53% Have seen an increase in their budget this year

65% Foresee an increase in their budget next year

2. What is at stake?

What is the biggest fear? And what are the biggest threats?

What is most valuable?

It's no surprise that customer information, financial information and strategic plans make up the top three most valuable information that organizations would like to protect.

Board member information and customer passwords follow closely after the top three listings. At the bottom of the top 10 list we find supplier information which shows that the ambition of "let us collectively protect the entire supply chain" still needs some work.

What are the biggest threats?

Most successful cyber breaches contain "phishing and/or malware" as starting points. Attacks focused on disruption rank in third place on the list, followed by attacks with a focus on stealing money.

Although there has been quite a lot of discussion about insider threats and state-sponsored attacks, the fear for internal attacks shows up as number eight on the list; espionage ranks bottom of the list.

> Importantly, more organizations are now beginning to recognize the broad nature of the threat. One thing that has changed for the better over the past 12 months, partly because of some of those big cyber attacks we've seen at a global level, is a growing realization that security is also about maintaining the continuity of business operations – and not only about the security of data and privacy."
>
> **Richard Watson**
> EY Asia-Pacific Cybersecurity Leader

Top 10 most valuable information to cyber criminals
1. Customer information (17%)
2. Financial information (12%)
3. Strategic plans (12%)
4. Board member information (11%)
5. Customer passwords (11%)
6. R&D information (9%)
7. M&A information (8%)
8. Intellectual property (6%)
9. Non-patented IP (5%)
10. Supplier information (5%)

Top 10 biggest cyber threats to organizations
1. Phishing (22%)
2. Malware (20%)
3. Cyberattacks (to disrupt) (13%)
4. Cyberattacks (to steal money) (12%)
5. Fraud (10%)
6. Cyberattacks (to steal IP) (8%)
7. Spam (6%)
8. Internal attacks (5%)
9. Natural disasters (2%)
10. Espionage (2%)

17%

Of organizations say their No. 1 fear is loss of customers' information

22%

See phishing as the biggest threat

2%

Rank espionage as a threat

3. Protection

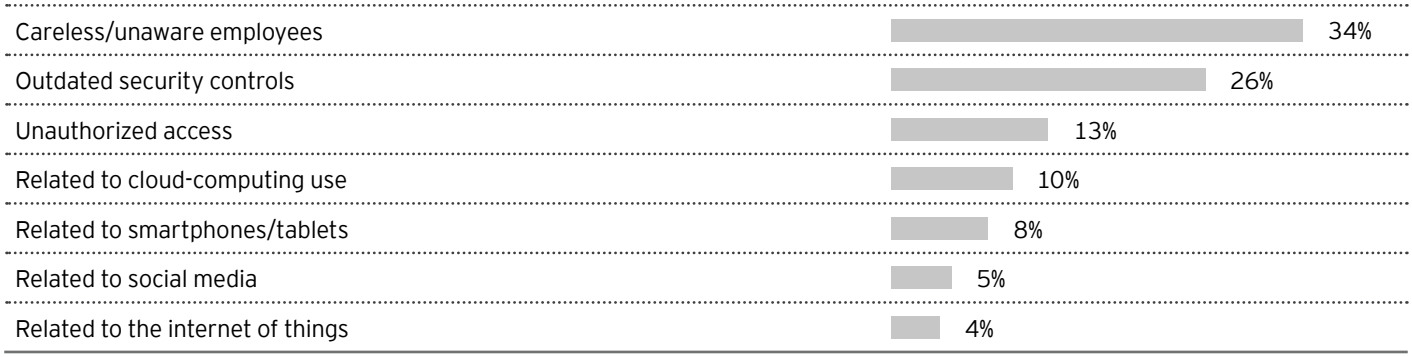
What are the riskiest vulnerabilities? How mature is cybersecurity?

Vulnerabilities increase when it comes to third parties. Only 15% of organizations have taken basic steps to protect against threats coming through third parties; 36% are aware of the risks through self-assessments (22%) or independent assessments (14%); therefore 64% have no visibility on this issue. Among smaller companies, this rises to 67%.

Larger companies are more mature than their smaller counterparts. For example, 35% have a formal and up-to-date threat intelligence program, compared with 25% of smaller organizations, and 58% say their incident response program is up to date, compared with 41% of smaller organizations.

> It's still taking many months to pick up sophisticated attacks. The challenge in this space is that identifying the right advanced threat detection and identification tools is difficult – organizations really struggle with the nuance of why one solution is more suitable than another. As a result, relatively few have implemented anything."
>
> **Dave Burg**
> EY Americas Cybersecurity Leader

Vulnerabilities with the most increased risk exposure over the past 12 months



34%

Of organizations see careless/unaware employees as the biggest vulnerability

53%

Have no program – or an obsolete one – for one or more of the following:

- Threat intelligence
- Vulnerability identification
- Breach detection
- Incidence response
- Data protection
- Identity and access management

4. Breaches

How are breaches identified?
How do organizations respond?

Organizations concede that they would be unlikely to step up their cybersecurity practices or spend more money unless they suffered some sort of breach or incident that caused very negative impacts.

A breach where no harm was caused would not lead to higher spending for 63% of organizations (in most cases harm has been done, but has not come to the surface yet). Many organizations are unclear about whether they are successfully identifying breaches and incidents. Among organizations that have been hit by an incident over the past year, less than a third say the compromise was discovered by their security center.

> The really smart and forward-thinking companies now have two budgets. They have their traditional budget for what they need to do and the projects they are pursuing, but they also have a contingency budget for unexpected eventualities such as the emergence of a new type of threat or a breach or compromise."
>
> **Dillon Dieffenbach**
> EY Japan Cybersecurity Leader

Breaches discovered by:

17%
Of organizations report a list of breaches in their information security reports

46%
Had no incidents (or don't yet know about them)

76%
Increased their cybersecurity budget after a serious breach

In the spotlight

Healthcare

The healthcare sector is having to store increasing quantities of personally identifiable and sensitive information. This year's GISS suggests that the sector's awareness of cyber risks is increasing, and many organizations are determined to put stronger protections in place. Progress has been made, but more work is necessary.

The healthcare sector has seen a number of cybersecurity incidents and alerts in recent months. In one incident, the health records of almost 100 million patients worldwide were put at risk by security bugs found in one of the world's most widely used patient and practice management systems.[10] In another, information such as the full names, dates of birth, insurance information, disability status, and home addresses of 2 million patients in Central America were exposed by a security failure.[11]

Healthcare data is extremely valuable on the "dark web", which makes healthcare organizations attractive to attackers. One in 3 US healthcare organizations have suffered a cyberattack, and 1 in 10 have paid a ransom.[12]

- **Governance.** Half of healthcare and Government & Public Sector organizations say they have increased spending on cybersecurity over the past 12 months, while 66% plan to spend more over the next 12 months.
- **What is at stake?** 17% of companies in the healthcare sector say that customers' personal and identifiable information is most valuable to cyber criminals, while 25% say that malware has most increased their risk exposure.
- **Protection.** Careless or unaware employees are seen by healthcare companies as the vulnerability that has most increased their risk exposure over the past 12 months (cited by 33%).
- **Breaches.** Only 18% of healthcare companies are very confident that they would be able to detect a sophisticated attack on their organization.

[10] "Health records put at risk by security bug", BBC News, August 7, 2018. [https://www.bbc.co.uk/news/technology-45083778]

[11] "Healthcare Data of 2 Million People in Mexico Exposed Online," Bleeping Computer, August 7, 2018. [https://www.bleepingcomputer.com/news/security/health-care-data-of-2-million-people-in-mexico-exposed-online/]

[12] "Survey Reveals More Than 1 in 3 Healthcare Organizations Have Suffered a Cyberattack While 1 in 10 Have Paid a Ransom," Business Wire, May 23, 2018. [https://www.businesswire.com/news/home/20180523005185/en/Survey-Reveals-1-3-Healthcare-Organizations-Suffered]

In the spotlight

Energy

The energy sector is an increasingly sophisticated user of emerging technologies, but this means it is facing more and more vulnerabilities in its information technology and operational technology. Successful attacks on this sector have the potential to cause devastating consequences, depriving communities of power and even jeopardizing citizens' safety.

There is plenty of evidence to show that energy companies are on the radar of cyber criminals — including the most sophisticated ones. In one recent case, security researchers found evidence of Russian hackers seeking to infiltrate US power companies.[13] In another, electricity companies were targeted in a spear phishing[14] scam thought to originate from North Korea.[15]

The threat has prompted regulators in Europe and elsewhere to look into new regulation to encourage the sector to focus on protecting enterprises.[16]

EY research suggests that energy companies now recognize these imperatives and are determined to protect themselves:

- **Governance.** Over half (57%) of energy companies have increased spending on cybersecurity over the past 12 months, and 68% plan to spend more over the next 12 months.
- **What is at stake?** 15% of companies in the sector regard customers' personal and identifiable information as most valuable to cyber criminals, but 14% say corporate strategic plans are; 27%, meanwhile, say that phishing has most increased their risk exposure.
- **Protection.** About 3 in 10 energy companies (29%) say that careless or unaware employees are the vulnerability that has most increased their risk exposure. About the same proportion (28%) cite outdated information security controls or architecture.
- **Breaches.** More than 4 in 10 energy companies (42%) say they have not had a significant cybersecurity incident in the past 12 months.

[13] "The worst cybersecurity breaches of 2018 so far," Wired, September 7, 2018. [https://www.wired.com/story/2018-worst-hacks-so-far/]

[14] "What is spear phishing?," Digital Guardian, April 16, 2018. [https://digitalguardian.com/blog/what-is-spear-phishing-defining-and-differentiating-spear-phishing-and-phishing]

[15] "Electricity industry on alert for cyber sabotage," Financial Times, November 8, 2017. [https://www.ft.com/content/1fc89bd8-996c-11e7-8c5c-c8d8fa6961bb]

[16] "New cybersecurity laws that the energy sector cannot ignore," Power Engineering International, February 27, 2018. [https://www.powerengineeringint.com/articles/2018/02/new-cybersecurity-laws-that-the-energy-sector-cannot-ignore.html]

03 Optimize cybersecurity

This year's GISS suggests that 77% of organizations are now seeking to move beyond putting basic cybersecurity protections in place to fine-tuning their capabilities.

These organizations are continuing to work on their cybersecurity essentials, but they are also rethinking their cybersecurity framework and architecture to support the business more effectively and efficiently. Part of that effort is considering and implementing artificial intelligence, robotic process automation, analytics and more to increase the security of their key assets and data.

Questions these organizations must focus on include:

- What is our cybersecurity strategy — what are our "crown jewels"
- What is our tolerance and appetite for risk?
- Are there any low-value activities we could do more quickly or more cheaply?
- How could technologies such as robotic process automation, artificial intelligence, and data analytics tools help us?
- Where do we need to strengthen our capabilities further?
- What can we stop doing, and how do we invest the resources we free up?

In this chapter, we look at the four vital components of optimizing cybersecurity:

1. **The status today.** To what extent is an organization's information security function currently able to meet its cybersecurity needs?
2. **Investment priorities.** Where is investment needed to update capabilities to the standard required?
3. **In-house or outsourced?** What is the best way to develop new cybersecurity capabilities and who should take the lead?
4. **Reporting.** How well is the organization able to evaluate its own capabilities and report back to key stakeholders?

At the moment, there is significant room for improvement. Fewer than 1 in 10 organizations say their information security function currently fully meets their needs — and many are worried that vital improvements are not yet under way.

Smaller companies are more likely to be lagging behind. While 78% of larger organizations say their information security function is at least partially meeting their needs, that falls to just 65% among their smaller counterparts.

Cyber criminals are raising their game, and the price of failure is high. In one recent attack, an Indian bank lost 944 million rupees (US$13.5m) after hackers installed malware on its ATM server that enabled them to make fraudulent withdrawals from cash machines.[17]

[17] "Indian bank loses $13.5m in global attack," Info Security, August 16, 2018. [https://www.infosecurity-magazine.com/news/indian-bank-loses-135m-in-global/]

1. The status today

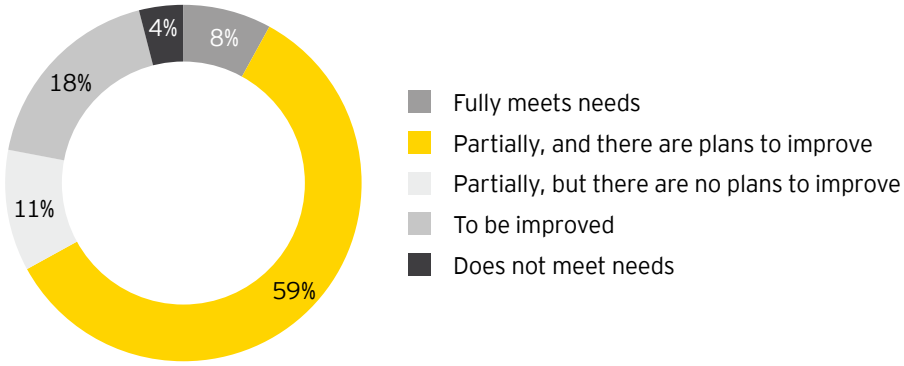
Is the information security function currently meeting the organization's needs? How serious is the shortfall?

Overall, 92% of organizations are concerned about their information security function in key areas. Resources are a key issue: 30% of organizations are struggling with skills shortages, while 25% cite budget constraints.

Smaller companies are especially concerned: 28% say their information security function does not currently meet their needs or is to be improved, and 56% say they have skills shortages or budget constraints.

> Some organizations may be overstating their resilience and security. Organizations may well have protection in parts, but the emerging cyber threat exists across many domains. The focus on enterprise security is one thing, but what about in the manufacturing and production environment, which might be digital or physical – and what about in the supply chain?"
>
> **Sean Wessman**
> EY Global Automotive and Transportation Cybersecurity Leader

Does the information security function meet the organization's needs?



8%

Of organizations have information security functions that fully meet their needs

38%

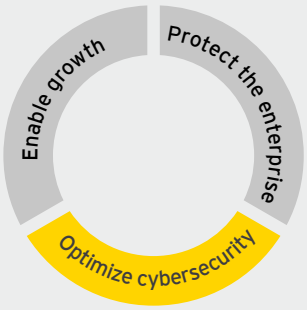
Would be unlikely to detect a sophisticated breach

51%

Are spending more on cyber analytics

2. Investment priorities

Where are the gaps?
Where are resources needed most urgently?

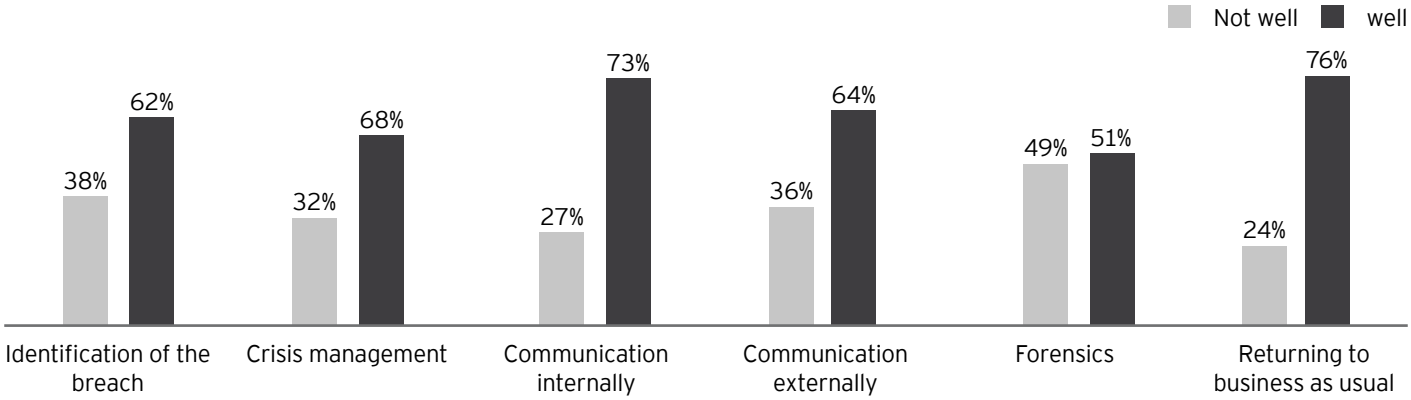


Better incident-response planning and execution is one important area where more organizations now need to optimize their capabilities. Forensics is a particular area of weakness, and this undermines organizations' ability to understand what has gone wrong and to improve protections.

Smaller companies are especially concerned: 39% say they are poor at identifying breaches, and 52% are worried about their forensics capabilities.

> Organizations need to look beyond preventive measures in their security assessments. A notable risk, based on our experience, is that many organizations have still not developed a robust cyber response plan."
>
> **Andrew Gordon,**
> EY Global Forensic & Integrity Services Leader

Priorities for improvement when a breach occurs: how organizations perform



35%

Of organizations have cyber insurance that meets their needs

<10%

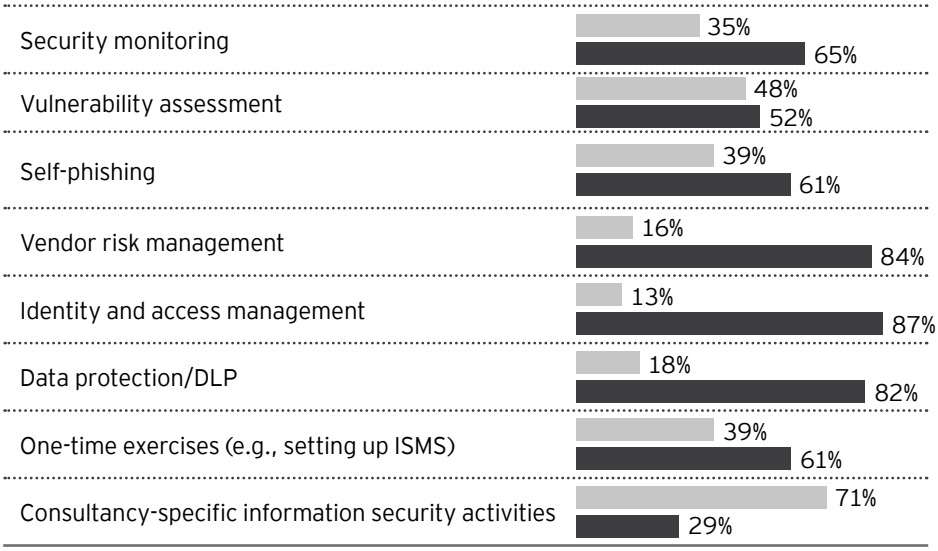
Believe they are mature on:

- Architecture
- Identity and access management
- Metrics and reporting
- Software security
- Third-party management
- Threat and vulnerability management

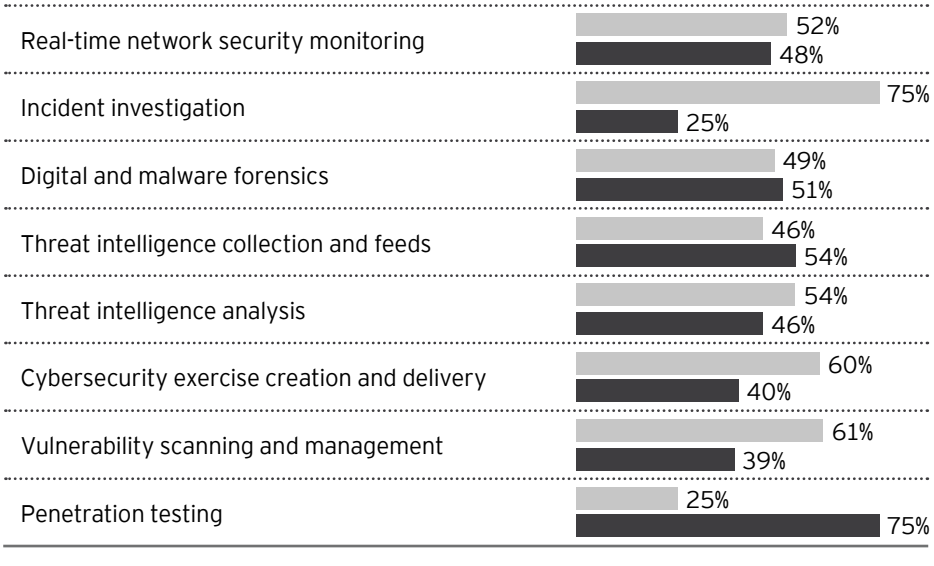
3. In-house or outsourced?

How do organizations improve their capabilities quickly? What should they do for themselves, and where do they need to look outside for help?

Which of the following security functions are you performing in-house or are you outsourcing?



Which functions of your security operations center are outsourced?



> The larger financial services organizations have introduced 'fusion' centers combining cybersecurity capabilities with multiple other competencies, such as the systems they use for anti-money laundering and know-your-customer. It's becoming a multi-disciplined endeavor that brings the business together across legacy and new systems."
>
> **Sundeep Nehra,**
> EY Americas Financial Services Cybersecurity Leader

72%

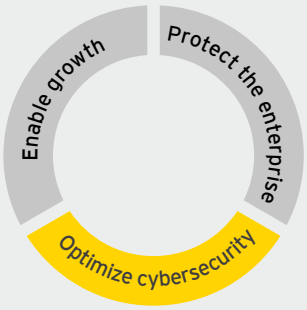
Of larger organizations have a security operations center

40%

Of smaller organizations have a security operations center

4. Reporting

Is the organization gathering information on cybersecurity capabilities and incidents? How is this being reported to stakeholders?

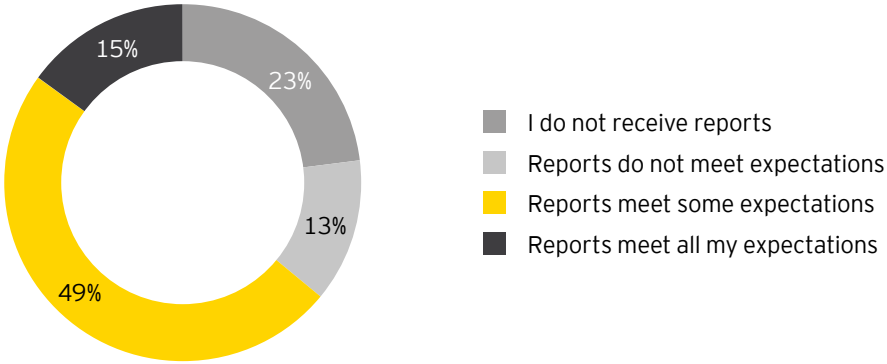


Only 15% of organizations say their information security reporting currently fully meets their expectations.

Smaller companies will need to move particularly quickly: almost a quarter (23%) do not currently produce information security reports, compared with 16% of larger organizations.

> The interest in cybersecurity reporting at board level has grown from attempts to understand technology to the point where boards now have a fiduciary responsibility to manage cybersecurity risk. Directors, shareholders and regulators are pressing for better reporting, even if organizations are not yet moving toward a posture of external disclosure."
>
> **Dave Padmos**
> EY Global Advisory Technology Sector Leader

Effectiveness of the organization's information security reports



20%
Of organizations cite the number of attacks in their information security reports

5%
Set out the financial impact of each breach

17%
Report on areas for improvement

In the spotlight

Consumer & Mobility

Consumer-facing companies face particular cybersecurity challenges. Maintaining trust is crucial to their businesses, but they are also especially vulnerable because they operate in a marketplace where customers require service 24 hours a day, seven days a week, through omni-channel business models. Cyber attackers exploit the weaknesses of these organizations because of the value and volume of consumer data that they could access.

In the meantime, the attacks keep coming. Some are familiar – such as the attack on British Airways that affected 380,000 transactions in September 2018.[18] Others are more sophisticated and unusual. For example, reports suggest that criminals are now selling a high-end phishing kit that enables attackers to target multiple online retailers.[19]

Our research suggests that consumer-facing organizations are making good progress on cybersecurity, but they must now refine their practices and develop more sophisticated defenses:

- **Current status.** Just 8% say their information security function currently meets the needs of the organization, and 29% warn that the function needs to be improved or does not meet their needs. Over half (55%) say they have plans to improve.
- **Investment priorities.** Consumer-facing companies point to significant gaps in their cybersecurity that need to be improved. More than 10% say their information security processes are either non-existent or very immature in the following areas: architecture, asset management, awareness, BCP and DR , incident management, policy and standards, security monitoring, software security, and third-party management.
- **In-house or outsourced.** About 4 in 10 consumer-facing companies (42%) have a security operations center, but many functions are widely outsourced. The majority of organizations in the sector outsource their security operation center's penetration testing (80%), threat intelligence collection and feeds (64%), real-time network security monitoring (60%), threat intelligence analysis (57%), and digital and malware forensics (53%).
- **Reporting.** Only 13% of consumer-facing companies say reports on information security meet all their expectations.

[18] "British Airways: suspect code that hacked fliers 'found'," BBC News, September 11, 2018. [https://www.bbc.co.uk/news/technology-45481976]

[19] "Researchers discover next generation phishing kit,", Help Net Security, April 25, 2018. [https://www.helpnetsecurity.com/2018/04/25/next-generation-phishing-kit/]

In the spotlight

Financial services

The financial services sector is at the heart of the battle against cyber attacks. Not only does it represent a hugely lucrative target for criminals, but it is also increasingly dependent on data.

The sector must keep that data secure at all costs — even as it adapts to initiatives such as open banking, which requires organizations to share data externally with trusted parties.

This work will need to accelerate, because attackers are continuing to target financial services organizations. Emerging technologies must take center stage: fake mobile banking apps now in circulation fool more than one in three consumers.[20] And more traditional scams continue. A new report on business email compromise fraud suggests that bank trojans are now in widespread use.[21]

To make matters worse, attackers are increasingly collaborating. In the summer of 2018, the FBI warned that criminals were planning a choreographed, multinational attack on the banking sector that drained ATMs of cash in hours.[22]

Our research suggests that financial services businesses have recognized that tension; protection is high (although continuous reflection and maintenance is necessary) and work on optimizing cybersecurity is underway:

- **Current status.** Only 6% of financial services companies say their information security function currently meets their organization's needs, but 65% have plans to make the required improvements. But there's a problem: 31% warn that skill shortages are a potential stumbling block.
- **Investment priorities.** Organizations in this sector are most concerned about the immaturity of their information security processes in the areas of architecture (cited as non-existent or very immature by 18%), metrics and reporting (18%), and asset management (17%).
- **In-house or outsourced.** Nearly 6 in 10 financial services organizations (59%) have a security operations center. They are more likely to run its functions in-house than outsourcing them: only penetration testing (79%) and forensics (52%) are outsourced by a majority.
- **Reporting.** While only 16% of financial services companies say that their reporting of information security meets their needs, that puts them ahead of other sectors.

[20] "Consumers falling for fake mobile banking apps," Info Security, February 27, 2018. [https://www.infosecurity-magazine.com/news/consumers-fake-mobile-banking-apps/]

[21] "Proofpoint warns of bank trojans," PYMNTS, August 8, 2018. [https://www.pymnts.com/news/b2b-payments/2018/proofpoint-report-bank-trojan-fraud-cybersecurity/]

[22] "FBI warns of choreographed ATM drainage," Naked Security, August 15, 2018. [https://nakedsecurity.sophos.com/2018/08/15/fbi-warns-banks-that-crooks-are-planning-choreographed-atm-drainage/]

04 Enable growth

1. Strategic oversight
2. Leadership
3. Digitalization
4. Emerging technologies

Organizations are going through a process of digital transformation. The nature of each transformation varies depending on the organization, but they will all have one or more of the following components: online sales/support to customers, supply chain integrations, application of robotic process automation, artificial intelligence, blockchain and analytics, business model disruption, and workplace innovation.

Organizations are now convinced that looking after cyber risk and building in cybersecurity from the start are imperative to success in the digital era. The focus now should also be on how cybersecurity will support and enable enterprise growth. The aim? To integrate and embed security within business processes from the start and build a more secure working environment for all. Security-by-design should be a key principle as emerging technologies move center stage.

To achieve these goals, organizations will need an innovative cybersecurity strategy rather than responding in a piecemeal and reactive way. The customer experience must be a key consideration.

Questions organizations must ask during their digital transformation:

- Is our entire supply chain secure?
- How do we design and build new channels that are secure by design?
- Where does cybersecurity fit into our digital transformation-enabled business model?
- Could strong privacy and data protection be a potential competitive differentiator?
- How focused on cybersecurity is our board as it pursues its digital ambitions for the organization?
- How are our most senior executives taking ownership of and showing leadership on cybersecurity?
- Do we have sufficient focus on cybersecurity in our entire eco-system?

In this chapter, we look at the four vital components of making cybersecurity part of the growth strategy:

1. **Strategic oversight.** To what extent do boards charged with pursuing digital transformation appreciate the need to build cybersecurity into their growth strategies?
2. **Leadership.** Who are digital organizations asking to take the lead on cybersecurity, and how is accountability delivered?
3. **Digitalization.** As organizations make greater use of digital technologies, how much does this increase cybersecurity vulnerabilities?
4. **Emerging technologies.** Where are organizations increasing investment in cybersecurity in order to build security-by-design?

Based on this year's survey, however, only a small number of organizations are concerned about the vulnerabilities to which emerging technologies are now exposing them. This is worrisome — not least because these technologies are also available to attackers. Security researchers at IBM have pointed to the potential for artificial intelligence to be used in developing malware: they developed a code called DeepLocker that can conceal its intent until after the target has been infected.[23]

But there is also good news. Many organizations now regard emerging technologies as a high priority for cybersecurity spending. That includes cloud, which is a much more established technology for most organizations, but also areas such as robotic process automation, machine learning, and artificial intelligence — and even the Internet of Things. Nonetheless, in most cases organizations do not yet intend to spend more on protecting themselves in these areas. Only cloud is marked out for additional spending by a clear majority of organizations.

[23] "DeepLocker — AI-powered malware are already among us," Security Affairs, August 9, 2018. [https://securityaffairs.co/wordpress/75206/malware/deeplocker-ai-powered-malware.html]

1. Strategic oversight

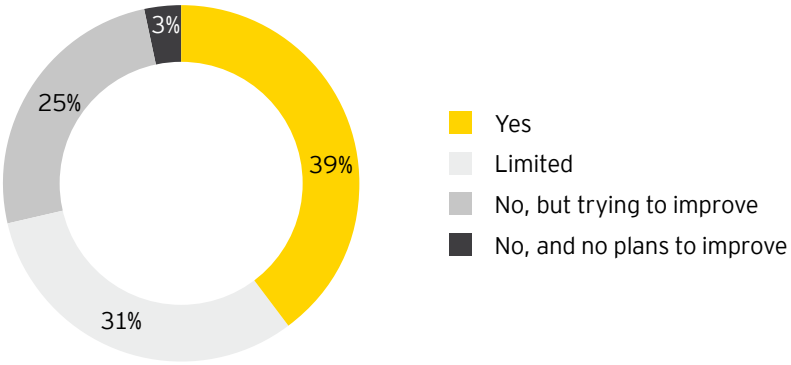
Does the organization have structures that make cybersecurity a key element of the board's strategic planning? Is good governance in place?

Some 70% of organizations say their senior leadership has a comprehensive understanding of security or is taking positive steps to improve their understanding.

However, larger organizations have made more progress: 73% have at least limited understanding, compared with 68% of their smaller counterparts.

> We need to see a rapid ramp-up of security-by-design. Many organizations are pursuing digital transformation at a breakneck pace, and there is a danger that cybersecurity is left behind. While it remains imperative to fix the organization's legacy systems, this must not be allowed to distract from building in strong protections from the start as emerging technologies are adopted."
>
> **James Phillippe**, EY Global Cyber Threat Management Leader

Does the board/executive management team have a comprehensive understanding of information security to fully evaluate cyber risks and preventive measures?



18%

Of organizations say that information security fully influences business strategy plans on a regular basis

55%

Say that information security influences business strategy plans somewhat or not at all

2. Leadership

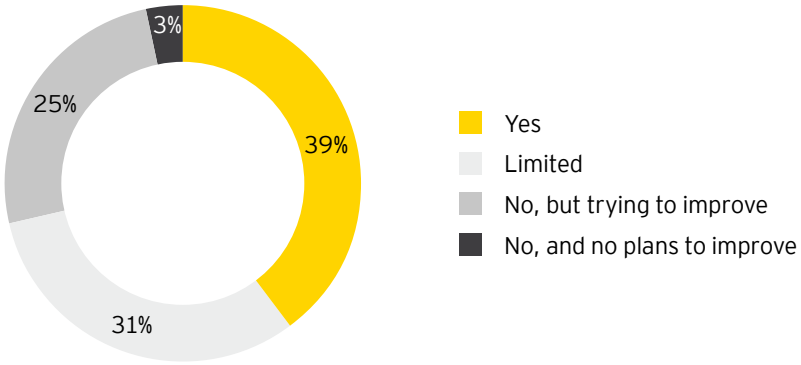
Who is ultimately accountable for cybersecurity? How do they show the leadership that drives leading practices across the organization?

The ultimate responsibility for information security is increasingly held at the most senior levels of the company. For 40% of organizations, the chief information officer (CIO) takes this responsibility.

Four in 10 organizations (40%) say that the person with ultimate responsibility is a member of the board or executive management. As security becomes a key enabler of growth, this proportion is likely to increase. Right now, smaller organizations are more likely to have information security accountability at board level than larger organizations.

> New types of roles are also emerging. We're now seeing the rise of the chief security officer (CSO). The CSO might be reporting to a chief information and security officer (CISO) or even a CIO, but he or she sits outside the CIO organization. They've got accountability for cyber risk, physical security risk, and personal security risk, while the CISO or CIO are the ones focused on broader cyber transformation."
>
> **Simon Adler**, EY Global Digital Identity & Access Leader

Does the board/executive management team have a comprehensive understanding of information security to fully evaluate cyber risks and preventive measures?



60%

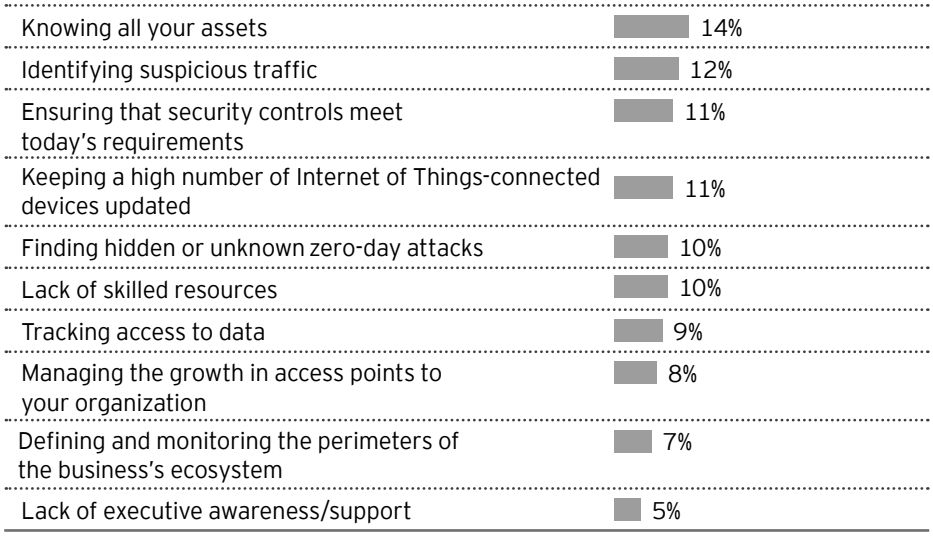
Of organizations say that the person directly responsible for information security is not a board member

3. Digitalization

As organizations pursue transformation, how does it increase their risk profile? What threats do new technologies pose?

Risks associated with growing use of mobile devices

Challenges related to the Internet of Things



8%

Of organizations say that smartphones have most increased their weaknesses

4%

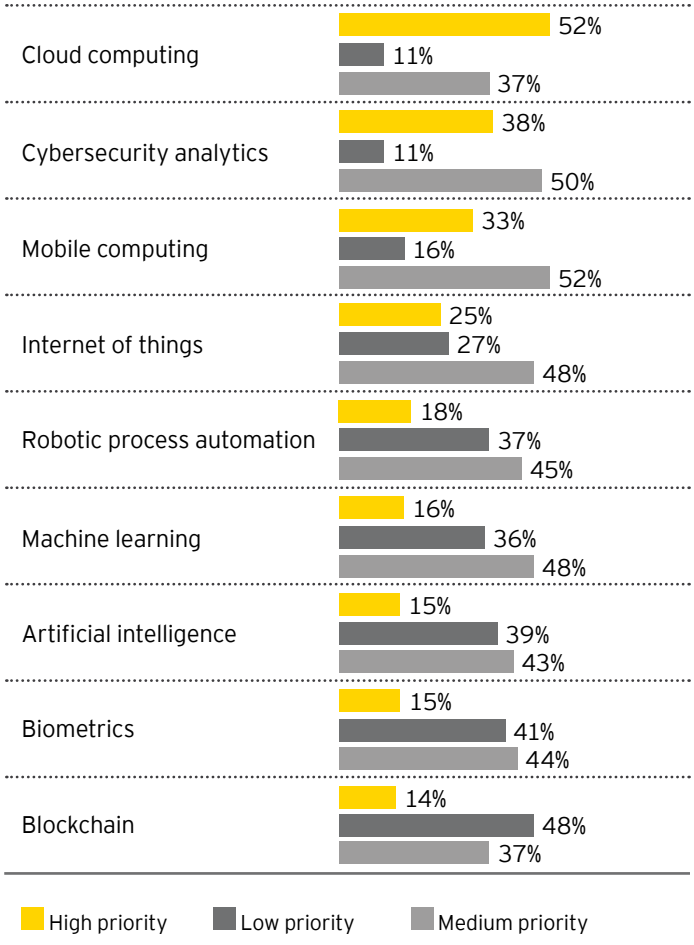
Are most concerned about the Internet of Things

> The value of data increases with its curation, so now is your chance to clean up your legacy information stores. As you integrate ecosystems with multiple suppliers, vendors and partners, there is an opportunity to build security into data management from the start. That opportunity is open to everyone."
>
> **Andy Ng**, EY EMEIA Information Protection Leader

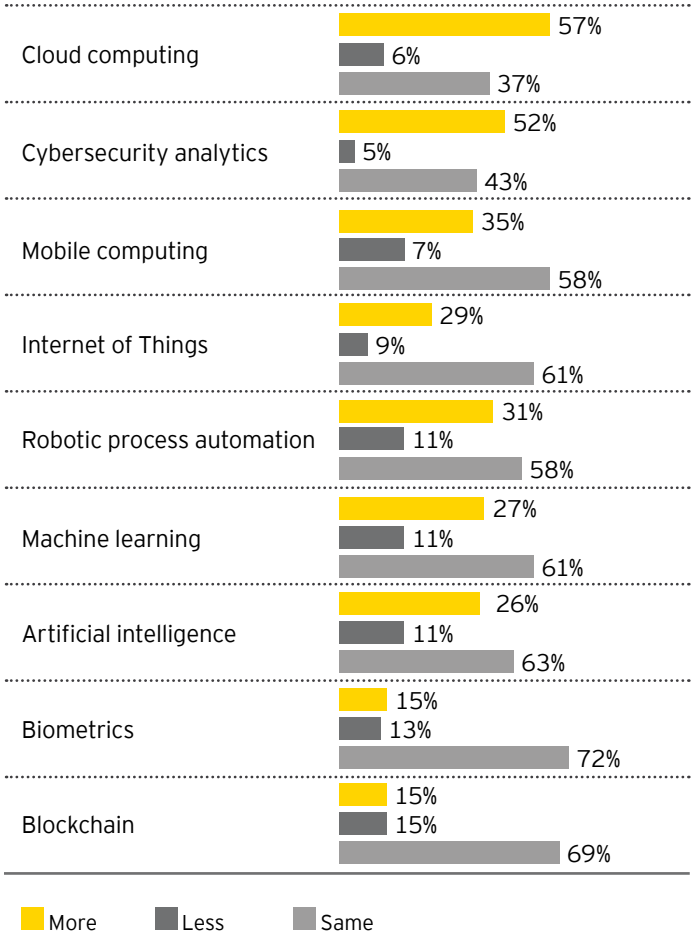
4. Emerging technologies

Where to prioritize investment from a cybersecurity perspective? How to promote security-by-design?

Priorities for cybersecurity investment this year



Spending compared to last year



> Those industries that are turning quickest to the digital opportunity must now spend the money on the cybersecurity side of things. They have to incorporate cybersecurity into the new architectures they're constructing – to take the opportunity to get rid of legacy systems that weren't built around protection and resilience."
>
> **Vinod Jayaprakash**, EY Cybersecurity Leader for Low-cost Delivery Centers

In the spotlight

Technology, Media & Entertainment and Telecommunications

Technology, Media & Entertainment and Telecommunications (TMT) organizations, which are so often at the forefront of disruption and transformation, may also be in a position to lead the way on cybersecurity.

But while start-up businesses with no legacy infrastructure have had an opportunity to embrace security-by-design from the start, that does not apply to all companies in the sector – many telecommunications organizations, for example, still operate assets installed decades ago.

Nevertheless, our research suggests that TMT businesses do recognize the importance of embedding cybersecurity into their growth strategies:

- **Strategic oversight.** Over half of TMT organizations (53%) say that information security fully influences their business strategy and plans.
- **Leadership.** At 47% of TMT companies, the person with direct responsibility for information security is on the board or is a member of the executive management team.
- **Digitalization.** 16% of the TMT organizations in the research say their risk exposure has increased the most by smartphones, Internet of Things technologies or social media over the past 12 months.
- **Emerging technologies.** Regarding new technologies, TMT organizations intend to increase their cybersecurity spending across the board. Cloud computing will be a particularly important focus, with 52% planning increased budgets.

Some threats to the TMT sector are indiscriminate — the chipmaker Taiwan Semiconductor, for instance, said in August 2018 that it had to stop production because of a variant of the WannaCry ransomware that has caused such damage across many industries.[24]

Other attacks are focused on technology companies' innovations. For example, both Google and Apple are fighting a constant battle to weed out apps from their Google Play and App Store respectively, with criminals offering malicious applications that masquerade as legitimate apps[25]; while messaging apps are increasingly being used to propagate phishing scams.[26] Elsewhere, Amazon moved quickly to shut down a flaw after researchers found a way to turn its Echo smart speaker into an eavesdropping device.[27]

[24] "Chip giant TSMC says WannaCry behind production halt," Security Week, August 6, 2018. [https://www.securityweek.com/chip-giant-tsmc-says-wannacry-behind-production-halt]

[25] "36 malicious apps advertised as security tools spotted in Google Play," SC Media, January 3, 2018. [https://www.scmagazine.com/home/news/cybercrime/36-malicious-apps-advertised-as-security-tools-spotted-in-google-play/]

[26] "Don't fall for this elaborate WhatsApp phishing scam," Trusted Reviews, February 12, 2018, [https://www.trustedreviews.com/news/new-whatsapp-scam-warning-adidas-trainers-free-3392920]

[27] "Researchers turn Amazon Echo into eavesdropping device," Bleeping Computer, April 25, 2018. [https://www.bleepingcomputer.com/news/security/researchers-turn-amazon-echo-into-an-eavesdropping-device/]

05 The results in summary – and action points for improvement

1. Protect the enterprise
2. Optimize cybersecurity
3. Enable growth

Protect the enterprise

	Summary	Next steps
Governance	Although investments in cybersecurity are on the rise and protection has improved across the board, successful cyber-attacks are increasing.	Cybersecurity needs to be in the DNA of the organization; start by making it an integral part of the business strategy.
What is at stake?	Phishing and malware underpin a large number of successful attacks; the GISS shows that organizations see them as the biggest threats.	Build awareness around phishing and malware – become 'click-smart'. Technology can help with phishing/malware email simulations.
Protection	Organizations are potentially connected with thousands of third parties; they are therefore more dependent on the security measures taken by those third parties.	Focus the security strategy and program on the entire eco-system of the organization: what threats will hurt us because of the lack of security at our third parties? Do we want to continue working with unsecure third parties? How can we help them?
Breaches	Most organizations increase their cybersecurity budget after they have experienced a breach. In most cases the breaches are not identified by the organization.	Increase cybersecurity budgets now (instead of after the fact) and focus the spend on threat detection and response. This will lower risk profiles significantly.

Optimize cybersecurity

	Summary	Next steps
The status today	Most organizations have cybersecurity functions that do not fully meet their needs; more than half of the organizations are investing in analytical capabilities as a first step.	Consider investments in analytical capabilities, especially when this enhances threat detection and improves awareness in the boardroom.
Investment priorities	Investments are necessary in many areas but above all in preparing for and dealing with a security breach. For many organizations, this is still a green field especially related to forensics.	It may be difficult to quickly build up forensic capabilities in house. Instead look to build a relationship with an outside vendor with these capabilities; have them available for when a breach occurs.
In-house or outsourced	Many organizations are currently outsourcing cybersecurity functions, including functions of their security operations centers.	Focus on where investment will be most effective, balancing the resources available inhouse with the capabilities of external suppliers.
Reporting	Most organizations are not satisfied with their reporting on security operations or security breaches.	Be more open around security operations (what we have done, where the gaps are, where we have breakdowns); this will help boost understanding of the threats and encourage the organization to take appropriate action.

Enable growth

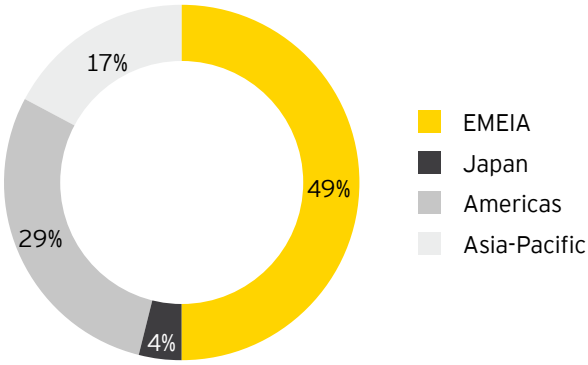
	Summary	Next steps
Strategic oversight	Strategic oversight is on the rise. The executive management in 7 of 10 organizations has a comprehensive understanding of cybersecurity or has taken measures to make improvements.	This is a huge step forward; put cybersecurity at the heart of corporate strategy.
Leadership	More board members are taking ultimate responsibility for cybersecurity, currently in 4 of 10 organizations.	Cybersecurity must be an ongoing agenda item for all executive and non-executive boards. Look to find ways to encourage the board to be more actively involved in cybersecurity.
Digitalization	The threats related to the use of smart phones, the Internet of Things and operational technology are not yet well understood. Only a small number of organizations name these areas as high risk areas.	Focus on cybersecurity as part of digital transformation strategy. The success of many digital projects will depend on establishing trust with customers.
Emerging technologies	The GISS shows many organizations are thinking about how emerging technologies can help with further optimizing cybersecurity. Priority and investments are well aligned.	Continue the focus on emerging technologies. Cyber criminals are also investing here, in artificial intelligence, for example. Resist the temptation to scale back investment in these key technology areas.

06 Survey methodology

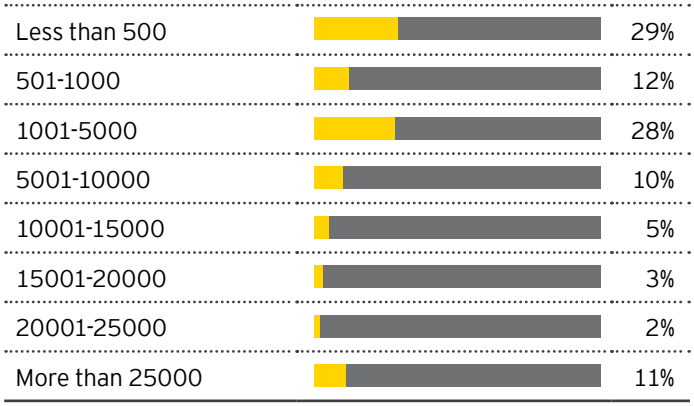
The 21st edition of *EY Global Information Security Survey* captures the responses of over 1,400 C-suite leaders and information security and IT executives/ managers, representing many of the world's largest and most recognized global organizations. The research was conducted between April-July 2018.

"Larger organizations" are defined in this report as organizations with annual revenues of US$1b or more. This group represents one-third of the total respondents to this survey. "Smaller organizations" are defined in this report as organizations with annual revenues below US$1b. This group represents two-thirds of the total respondents to this survey.

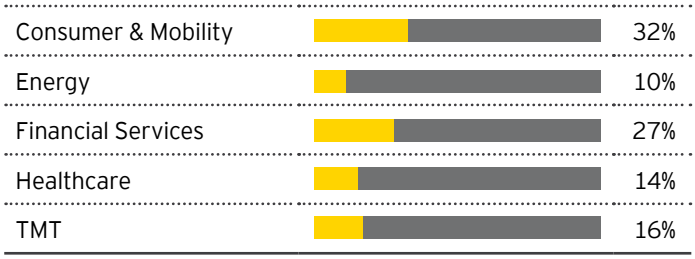
Respondents by area



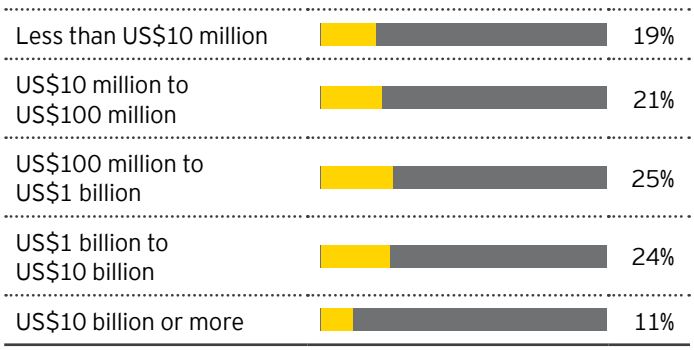
Respondents by number of employees



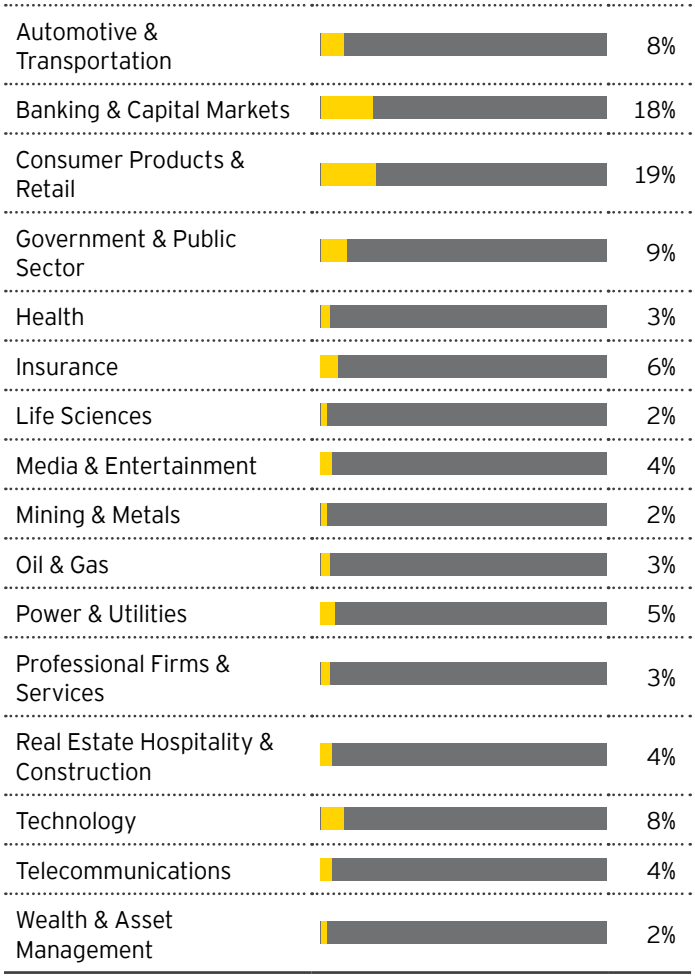
Respondents by industry sector cluster



Respondents by total annual revenue (in USD)



Respondents by industry sector



The Consumer & Mobility cluster includes respondents from Automotive & Transportation, Consumer Products & Retail and Real Estate Hospitality & Construction sectors. The Energy cluster includes respondents from Mining & Metals, Oil & Gas and Power & Utilities sectors. The Financial Services cluster includes responses from Banking & Capital Markets, Insurance and Wealth & Asset Management sectors. The Healthcare cluster includes responses from Government & Public Sector, Health and Life Sciences sectors. The TMT cluster includes respondents from Technology, Media & Entertainment and Telecommunications sectors.

Global

Paul van Kessel
+31 88 40 71271
paul.van.kessel@nl.ey.com

Andrew Gordon
+44 20 7951 6441
Andrew.Gordon@uk.ey.com

Americas

Dave Burg
+15716333628
Dave.Burg@ey.com

Brian Loughman
+12127735343
brian.loughman@ey.com

Asia-Pacific

Richard Watson
+61 2 9276 9926
richard.watson@au.ey.com

Emmanuel Vignal
+86 21 2228 5938
emmanuel.vignal@cn.ey.com

EMEIA

Mike Maddison
+44 20 7951 3100
mike.maddison@uk.ey.com

Jim McCurry
+44 20 795 15386
jmccurry@uk.ey.com

Japan

Dillon Dieffenbach
+81 3 3503 1490
dillon.dieffenbach@jp.ey.com

Ken Arahari
+81 3 3503 1110
ken.arahari@jp.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY's Advisory Services

EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions, create innovative answers and realize long-lasting results.

The better the question. The better the answer. The better the world works.

EYG no. 011483-18Gbl

ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com