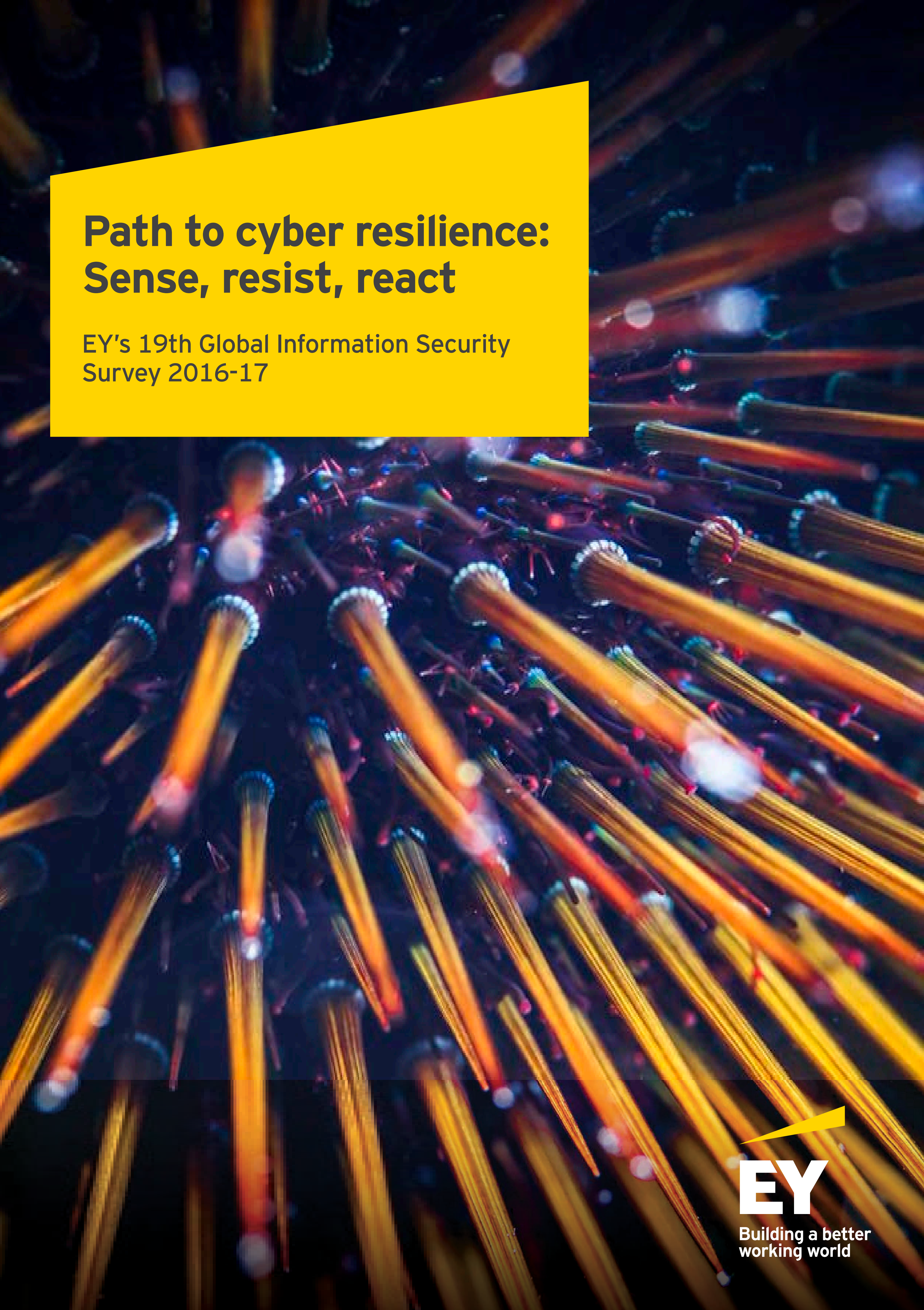
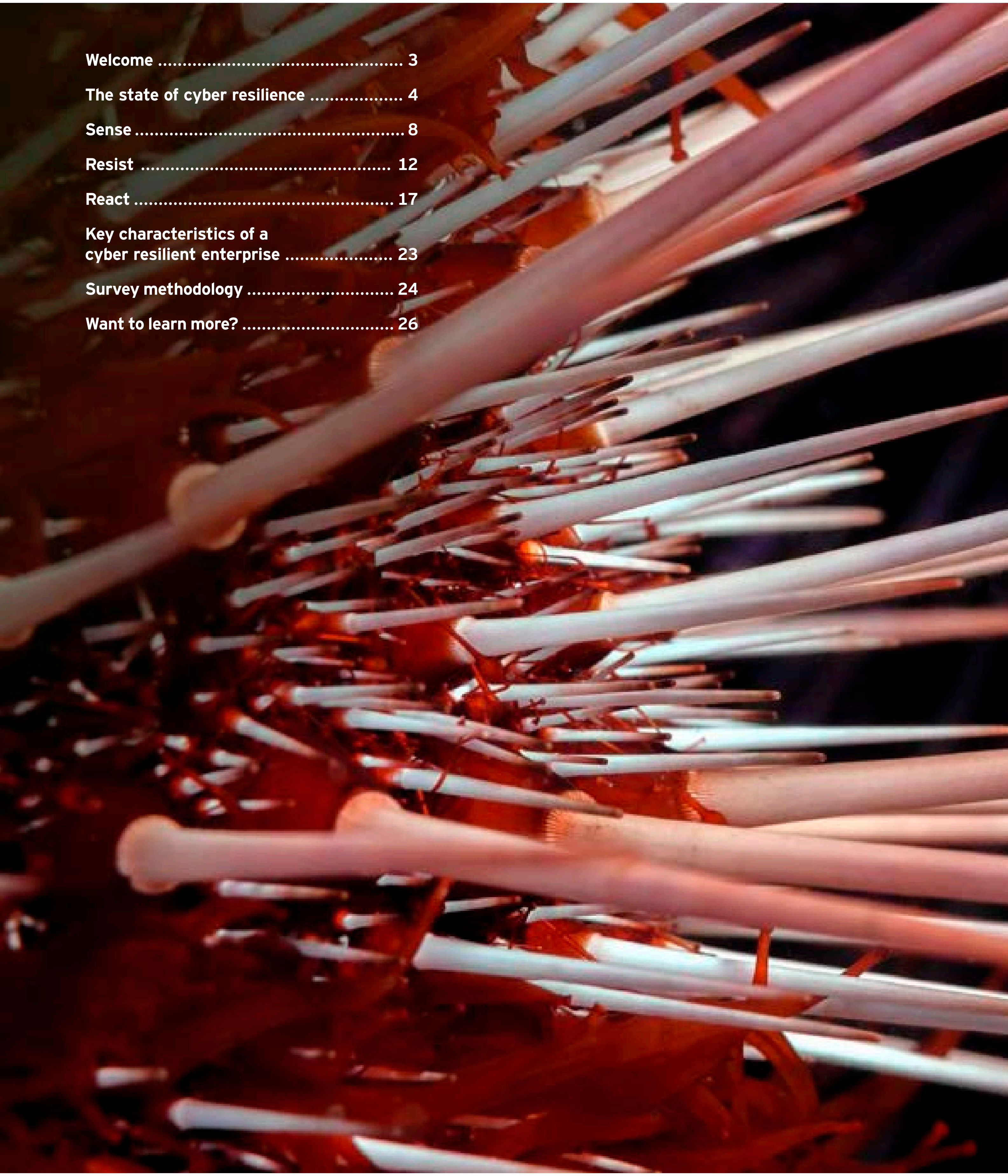


Path to cyber resilience: Sense, resist, react

EY's 19th Global Information Security Survey 2016-17

Building a better working world

Contents



Welcome

Whenever I talk to boards, executives or CIOs, there is always a lot to talk about on cybersecurity. Is our cybersecurity working and is it doing the right things? They worry about having enough budget, a team with the right skills and latest technologies, and above all, they really worry about suffering a major cyber attack despite everything they have done to prevent one. The truth is, everyone needs help. Since we are all facing the same "common enemy," the more we share about our concerns and experiences, our successes and failures, and the more we collaborate on finding answers, then the more we will learn and together we will be better protected.

There are some things we know for certain. Cybersecurity is a shared responsibility across the organization. The board needs to support the efforts being made, and every employee needs to learn how to stay out of trouble and not open the phishing email, or lose their mobile device. But even if you have all this, does it make you feel wholly confident?

We might not want to admit it, but probably not. Because if there is something else you know, it is that the devil is in the detail, and when you think about the cybersecurity you need across your entire ecosystem, there is a lot of detail.

In this report, we look at the findings of our latest *Global Information Security Survey*. From looking at the responses of the 1,735 CIOs, CISOs and other executives who generously shared their information, we can see where organizations are in the strength and maturity of their cybersecurity capabilities and we believe there are some very specific things organizations can do.

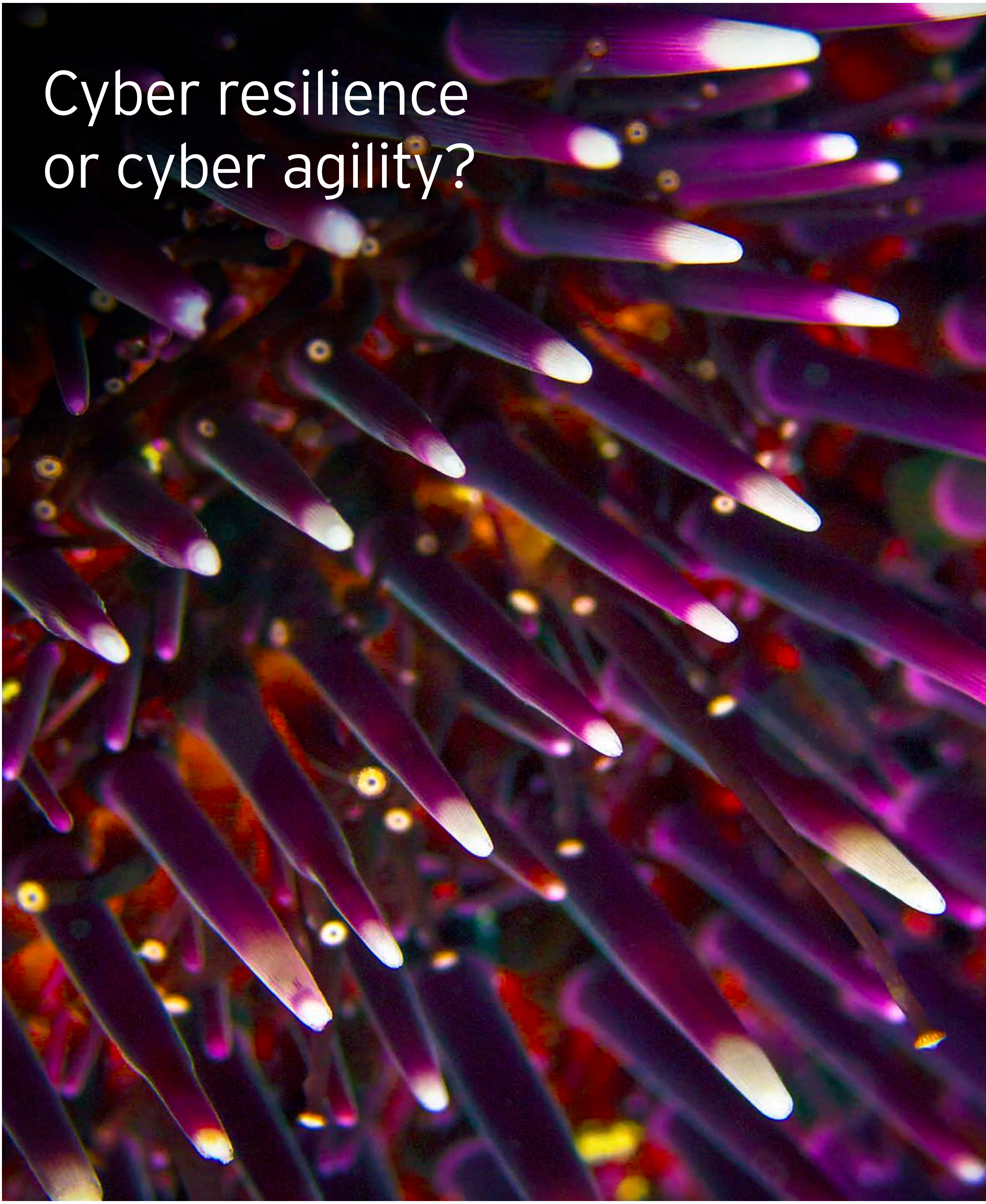
- **First, sharpen your senses.** Can you see the cyber attacker approaching your perimeter? Does your perimeter even exist anymore? Would you know if someone is beginning to undermine – or launch an attack over – your defenses? Could you spot an attacker hiding in a remote part of your network?
- **Second, upgrade your resistance to attacks.** What if the attack was from a new, more sophisticated technique that you haven't experienced before? Would your defenses be able to resist something new and more powerful?
- **Third, react better.** In the event of a cyber attack, what is the organization's plan and what is your role in it? Are you going to focus on quickly repairing the damage or will you be painstakingly collecting evidence for law enforcement? What would be the first thing you would do?

There are a lot of positives. We've come a long way in a short time and are doing a good job, it's just that we have to keep doing it better as our enemy comes up with newer tricks. So while the three sections of this report: Sense, Resist and React, might give you something to work on in your organization, we should also stay connected so we can share and learn. Let's continue to help each other out.

Paul van Kessel

EY Global Advisory Cybersecurity Leader
paul.van.kessel@nl.ey.com

The state of cyber resilience



Cyber resilience or cyber agility?

Threats of all kinds continue to evolve, and today's organizations find that the threat landscape changes and presents new challenges every day. In response, organizations have learned over decades to defend themselves and respond better, moving from very basic-level measures and ad hoc responses to sophisticated, robust and formal processes. Key events such as the increase in digital innovation, expansion of connected products, the Sarbanes-Oxley Act, changing regulatory landscape, repeated financial crises, catastrophic product failures, terrorist attacks and the explosion in cybercrime are just a few examples of why organizations needed to evolve their defensive and protective measures. Here is a short overview of that evolution:

1970s	1980s	1990s	2000	2010
‣ Ready for natural hazards ‣ Physical response measures in place, e.g., evacuation and first aid ‣ Call for external assistance	‣ Reliance on a few new technologies ‣ Basic disaster recovery in response to system failures ‣ Virus protection developed ‣ Identity and access management	‣ Enterprise-wide risk management introduced ‣ Regulatory compliance commonplace ‣ Business continuity a focus	‣ Advances in information & cybersecurity ‣ Switch to online ‣ Third-party outsourcing, e.g., cloud ‣ Connectivity of devices	‣ Global shocks (terrorist, climate, political) ‣ Business resilience ‣ Internet of Things (IoT) ‣ Critical infrastructure ‣ State-sponsored cyber espionage and cyber attacks
Mainframes	**Client/Server**	**Internet**	**E-Commerce**	**Digital**

Cyber resilience is a subset of business resilience; it is focused on how resilient an organization is to cyber threats. Before going into the details, let us first look at the three high-level components of cyber resilience and how well – in general – organizations are performing in these three areas:

Sense

Sense is the ability of organizations to predict and detect cyber threats. Organizations need to use cyber threat intelligence and active defense to predict what threats or attacks are heading in their direction and detect them when they do, before the attack is successful. They need to know what will happen, and they need sophisticated analytics to gain early warning of a risk of disruption.

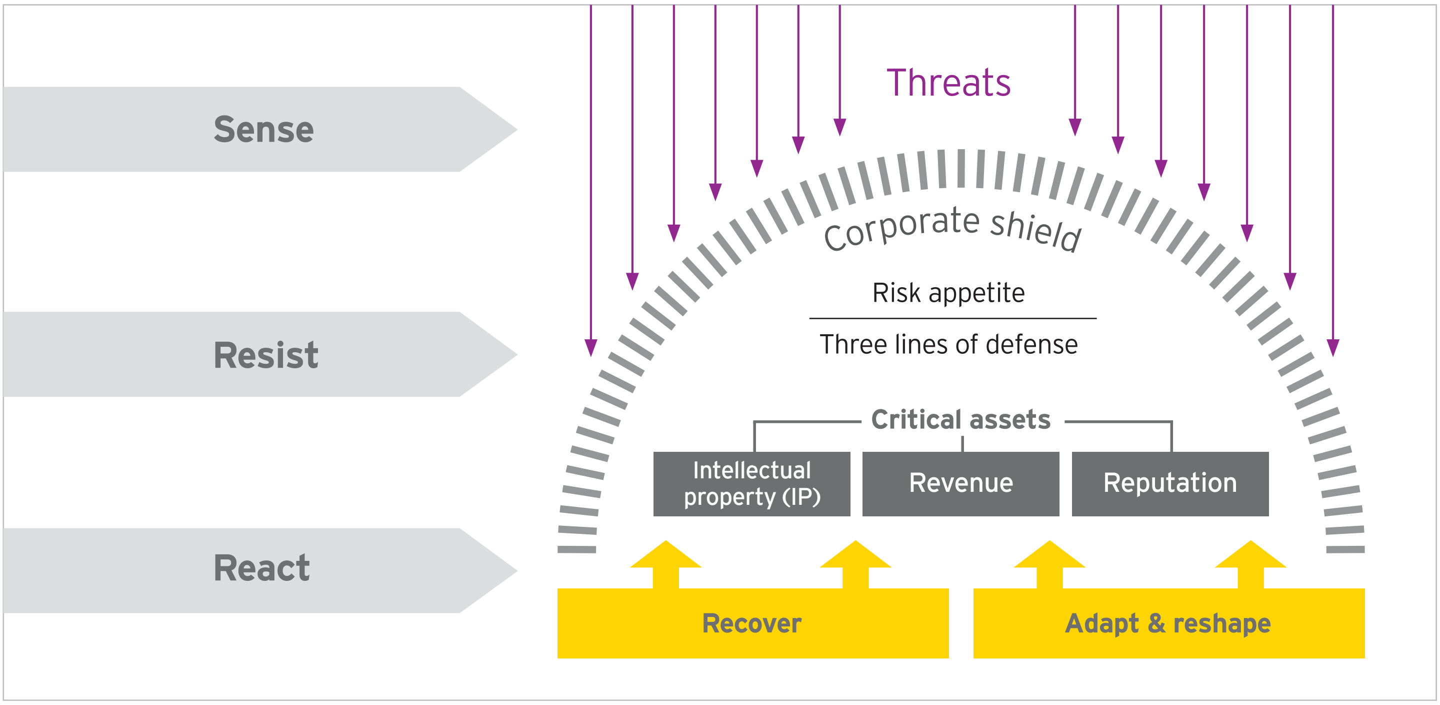
Resist

Resist mechanisms are basically the corporate shield. It starts with how much risk an organization is prepared to take across its ecosystem, followed by establishing the three lines of defense:

1. First line of defense: Executing control measures in the day-to-day operations
2. Second line of defense: Deploying monitoring functions such as internal controls, the legal department, risk management and cybersecurity
3. Third line of defense: Using a strong internal audit department

React

If Sense fails (the organization did not see the threat coming) and there is a breakdown in Resist (control measures were not strong enough), organizations need to be ready to deal with the disruption, ready with incident response capabilities and ready to manage the crisis. They also need to be ready to preserve evidence in a forensically sound way and then investigate the breach in order to satisfy critical stakeholders – customers, regulators, investors, law enforcement and the public, any of whom might bring claims for loss or noncompliance. If the responsible parties are identified, the organization might initiate a claim against them. Finally, they also need to be prepared to bring the organization back to business as usual in the fastest possible way, learn from what happened, and adapt and reshape the organization to improve cyber resilience going forward.



The overall picture

Before we explore in more detail, let us first paint a picture of the overall status of cyber resilience. At a high level, the message is positive: organizations are moving in the right direction. Over recent years and under the pressure of more regulation, organizations have invested in their corporate shield. Significant progress has been made in taking measures to strengthen this shield and in the last two to three years, we have also seen organizations focus more on their Sense capabilities. Most organizations however are lagging behind in preparing their reaction to a breach, still ignoring the all-too-familiar statement, "it's not a matter of 'if' you are going to suffer a cyber attack, it's a matter of 'when' (and most likely you already have been)."

We have summarized the overall picture, and in the next sections of this report, we will explore the components of cyber resilience in more detail.

	Sense (See the threats coming)	**Resist** (The corporate shield)	**React** (Recover from disruption)
Where do organizations place their priorities?	**Medium**	**High**	**Low**
Where do organizations make their investments?	**Medium**	**High**	**Low**
Board and C-level engagement	**Low**	**High**	**Low**
Quality of executive or boardroom reporting	**Low**	**Medium**	**Low**

Cyber resilience or cyber agility?

People taking a flight nowadays can be quite impressed by how quickly the airlines have incorporated new security measures related to charging smartphones during the flight. In the cybersecurity space, there is a similar desire. Organizations would like to respond to changes as quickly as possible. Questions like "How can I increase the agility of my cybersecurity?" and "How can I quickly respond to what is happening in cyberspace?" are often heard.

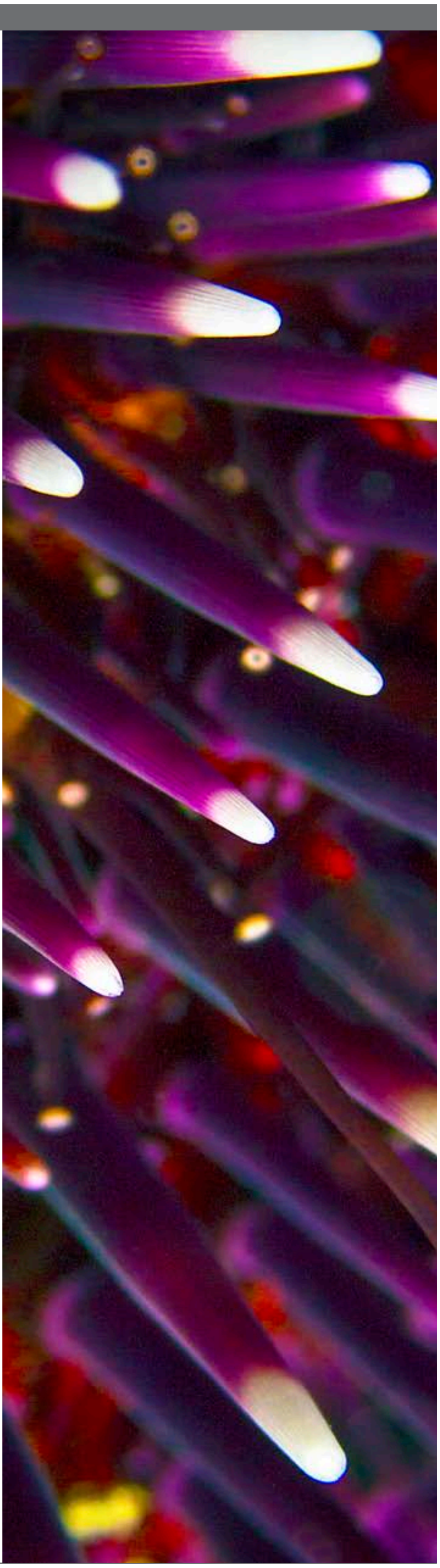
Organizations want to know how to predict the next threat, and what the "hottest" thing available to prevent it is. Cyber threat intelligence, cyber threat management and related software, consulting and implementing new tools have become priorities in most organizations. All with the intent to increase cyber agility, which is the ability to react to a change in the threat landscape.

Aiming for more cyber agility is great, and investing money in that direction is well spent. However, the main question organizations should ask is: "Are you cyber resilient?" In other words, is your cybersecurity capability as a whole strong enough to mitigate all the cyber risks the company is facing? Cyber resilience is not only a matter of responses to new technology and new threats; if it only focuses on responses, that may result in ad hoc security measures which do not create the stable foundation that a mature cybersecurity capability needs.

Year after year, our EY *Global Information Security Survey* shines a spotlight on the cybersecurity issues that are most troublesome to businesses. Over the last two years, 87% of board members and C-level executives have said that they lack confidence in their companies' level of cybersecurity. So there is still a lot to do. Attention for cyber agility is a must – but let us not get blindsided and think that cyber agility automatically results in a positive answer to the main boardroom question of "Are we cyber resilient?"

87%

of board members and C-level executives have said they lack confidence in their organization's level of cybersecurity.



Sense

A high level of confidence?

Organizations have improved their Sense capabilities significantly in recent years. Many organizations are using cyber threat intelligence to predict what they can expect, installing continuous monitoring mechanisms, such as a security operating center (SOC), identifying and managing vulnerabilities, and installing active defense. They have become more confident in their ability to predict and detect a sophisticated cyber attack; this year, 50% of organizations thought it was likely they would be able to do so, which is the highest level of confidence we have seen since 2013.

But against these positives are the simple facts that, according to our survey, not enough organizations are paying attention to what today should be the basics, and everyday these organizations are putting their customers, employees, vendors and ultimately their own future at considerable risk. That there is still work to do, related to the basic Sense capabilities, is witnessed by the following findings in this year's survey:

- Forty four percent do not have a SOC.
- Sixty four percent do not have, or only have an informal, threat intelligence program.
- Fifty five percent do not have, or only have an informal, vulnerability identification capability.

In addition to these basics, there are four specific areas that need special attention, and which could force an organization to rethink what it is doing.

44%

do not have an SOC.

64%

do not have, or only have an informal, threat intelligence program.

A breach has happened, but there appears to be no harm

Of the organizations in our survey, 62% would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm. In most cases, there is harm being done, but there was no immediate evidence found to support that. Cyber criminals often make "test attacks," lie dormant after a breach, or use a breach as a diversionary tactic to throw organizations off the trail of what they are really up to. Organizations should assume that harm has been done every time there is an attack, and if they have not found it, they should consider that they have not found it yet.

62%

would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm.

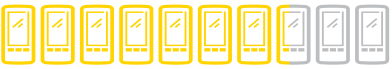
Securing your ecosystem

In our digital and connected world, events in the organizations' network of suppliers, customers, government bodies, etc. (the ecosystem), can still go on to impact the organization itself. This is a major area of risk which is often overlooked, as evidenced by the following findings:

- Sixty eight percent of responders would not increase their information security spending even if a supplier was attacked – even though a supplier is a direct route for an attacker into the organization.
- Fifty eight percent would not increase their spending if a major competitor was attacked – although cyber criminals like to attack organizations that are similar in infrastructure and operating frameworks, and they carry forward the learnings from one successful attack to the next.

An organization's sensory system is much stronger when events in the surrounding ecosystem are taken into account.

73%



are concerned about poor user awareness and behavior around mobile devices.

49%

doubt that they are going to be able to continue to identify suspicious traffic over their networks.

The impact of the IoT

The emergence of the Internet of Things and the explosion in the number of connected devices is going to put more pressure on the Sense capabilities of an organization. The following are just some of the challenges this creates for organizations:

- **Challenges related to the number of devices**

  Organizations are struggling with the huge number of devices that will become part of their networks in a very short period of time. Our findings show 73% are concerned about poor user awareness and behavior around mobile devices. Too many organizations are also concerned about their ability to know all their assets (46%), how they are going to keep these devices bug free (43%), how they will be able to patch vulnerabilities fast enough (43%) and about their ability to manage the growth in the access points to their organization (35%).

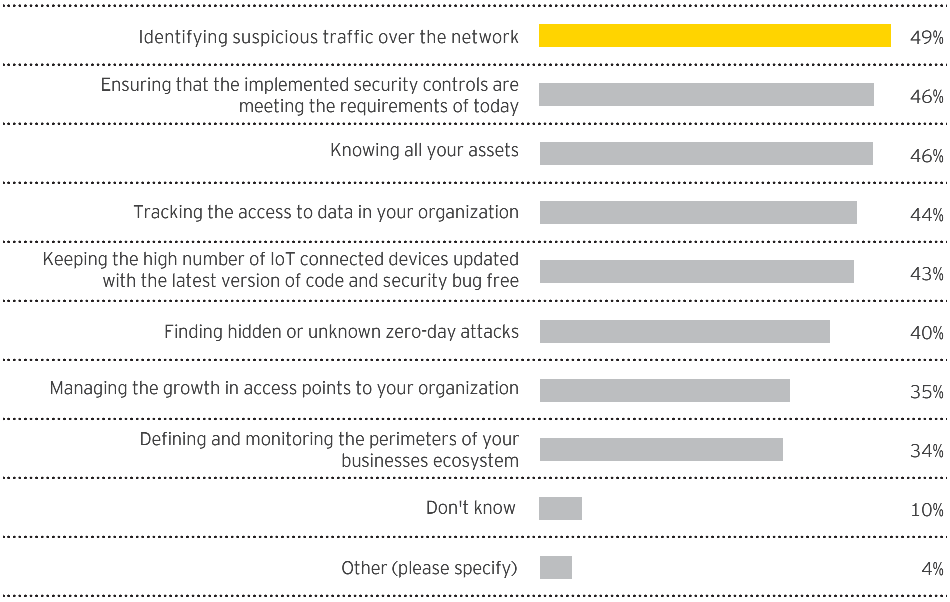
- **Challenges related to the size of the data traffic**

  Organizations doubt that they are going to be able to continue to identify suspicious traffic over their networks (49%), to track who has access to their data (44%) or to be able to find hidden and unknown zero-day attacks (40%).

- **The challenges related to the ecosystem**

  The ecosystem is going to grow significantly as connectivity to other organizations expands, and the volume of data it exchanges increases. It will become more and more difficult to identify what part of the ecosystem is going to impact the organization and what is not, and it will be doubly difficult if the organization's own cybersecurity is fragmented and not joined up. As a result, many organizations expect difficulties with monitoring the perimeter of their ecosystems (34%).

What do you consider to be the information security challenges of the IoT for your organization? (Select all that apply)



Information sharing and collaboration are on the rise

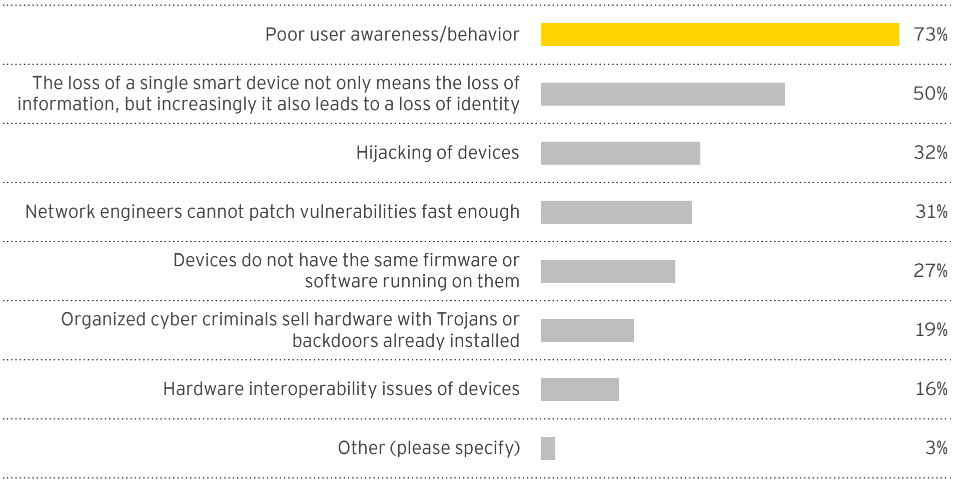
Governments and other entities are all increasingly concerned with your cybersecurity. Industry-specific regulations relating to cyber risks are gathering momentum, and legislative interest is increasing. So new regulations and laws should be expected. In many parts of the world, standards are being developed for critical infrastructure organizations, and there are calls for greater information sharing and collaboration, as well as mandatory reporting of cyber attacks, so that cybercrime can be fought together. It should be anticipated that this will become compulsory, and even if it does not happen in the short term, the atmosphere today will lead regulators, stakeholders, business partners and even customers to want to know more about your cybersecurity. So be prepared to report and look for opportunities to share and collaborate today. Currently our survey revealed the following:

- Forty nine percent of our respondents' SOCs collaborate and share data with others in the same industry.
- Thirty eight percent of our respondents' SOCs collaborate and share data with other public SOCs.

49%

of our respondents' SOCs collaborate and share data with others in the same industry.

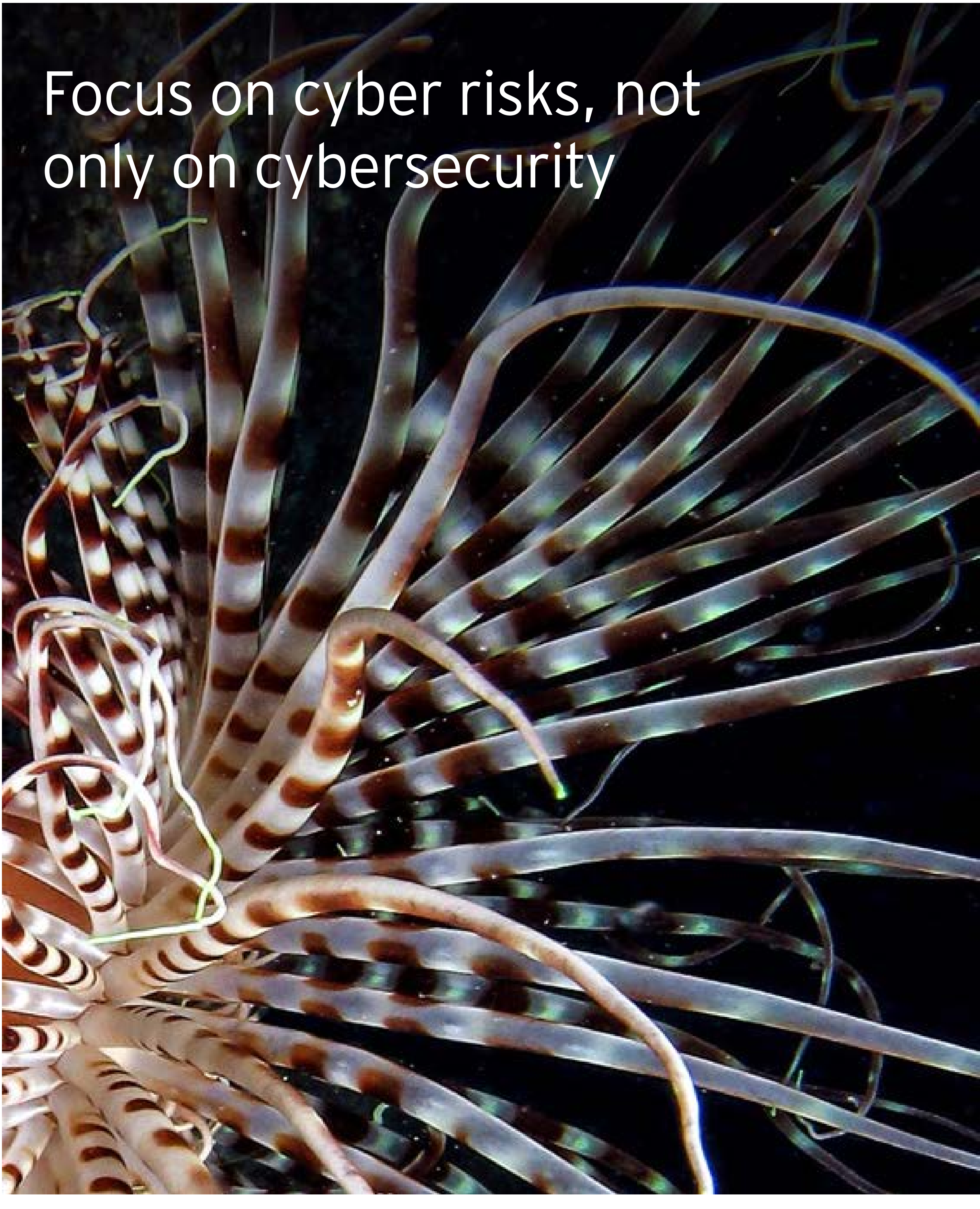
What are the main risks associated with the growing use of mobile devices (e.g., laptops, tablets, smartphones) for your organization? (Select all that apply)



Today's cyber criminals can be ruthless, and their behavior and methods are almost impossible to predict.

Cyber criminals — like other organized criminals — are prepared to behave in ways that most of us cannot understand. Their actions convey a different set of values, ethics and morality, and they are often driven by motivations that are hard to fathom. Apart from the more usual and expected fraud and theft, consumers increasingly have fears about cars being hacked into to cause accidents, and some critical infrastructure organizations are seeing cyber ransom become a reality. Such is the creativity of the criminal networks that they will always find new ways to launch attacks for personal profit, or to achieve headlines for a cause. Sense, Resist and React have a fundamentally important part to play in protecting the cyber ecosystem, especially with the growth of the IoT. Without effective cybersecurity many organizations and governments are not just risking their data and IP, they may be putting individuals at risk, and in the future, we should expect to see even more collateral damage.

Resist



Focus on cyber risks, not only on cybersecurity

Generally, organizations have greatly improved their abilities to resist attacks, and many organizations can say they are successfully defending against thousands of attacks every day. But attacks take many different and increasingly complex forms and while executing the control measures in the corporate shield may work against simple Distributed Denial of Service or viruses, it is not performing as well as it should against the sophisticated, persistent attacks that the dedicated and organized cyber criminals are launching against their targets every day.

- Last year, 88% of respondents to our survey said that their cybersecurity function did not fully meet their organization's needs. This year it is 86%, which does not represent a significant improvement. Despite the steps organizations have taken, it is still not enough to deal with the worsening situation.

86%

say their cybersecurity function does not fully meet their organization's needs.

Focus on cyber risks, not only on cybersecurity

In our 2016 survey, nearly half (48%) of responders say that their outdated information security controls or architecture is a high area of vulnerability, consistent with results from 2013 and 2014, whereas in 2015 only 34% rated this as a high area of vulnerability. Overall, 2015 saw a significant surge in confidence with organizations seeing many vulnerabilities and threats as less of a challenge than in previous years. That confidence in being able to resist attacks has been short-lived in the face of the growth in employee-related risks and threats and the increased knowledge of how criminal syndicates are specifically targeting this human weakness. This year there is a significant upswing in how they rate their risk exposure. In 2015, organizations appeared to think they had begun to solve the problem of cybersecurity and they were better able to resist attacks, only to be caught out, or to simply become more aware of the threats.

Which threats and vulnerabilities have most increased your risk exposure over the last 12 months?

The chart shows a total percentage figure for those items rated 1 (highest) and 2 (high), from 2013–16.

	2013	2014	2015	2016
Vulnerabilities				
Careless or unaware employees	53%	57%	44%	55%
Outdated information security controls or architecture	51%	52%	34%	48%
Unauthorized access	34%	34%	32%	54%
Threats				
Malware	41%	34%	43%	52%
Phishing	39%	39%	44%	51%
Cyber attacks to steal financial information	46%	51%	33%	45%
Cyber attacks to steal IP or data	41%	44%	30%	42%
Internal attacks	28%	31%	27%	33%

57%

of responders have had a recent significant cybersecurity incident.

Where should organizations focus to better resist today's attacks?

Activate your defenses

While the nature of the attacks has changed, resisting, defending, mitigating and neutralizing attacks has long been the necessary core of cybersecurity. The services and tools an organization can use to resist have mostly kept pace, and many highly effective solutions are available today. Nevertheless our survey reveals that 57% of responders have had a recent significant cybersecurity incident, which shows that there is still more work to do to strengthen the corporate shield. Maturity levels are still too low in many critical areas, and improving each would be a significant step forward for any organization.

Percentage of respondents who would rate these information security management processes as mature:

- Software security: 29%
- Security monitoring: 38%
- Incident management: 38%
- Identity and access management: 38%
- Network security: 52%

Take an unorthodox approach

The ability to resist requires a multifaceted approach. Defenses are usually seen as hard barriers, like encryption, or firewalls that stop and neutralize an attack, but there are other ways organizations can minimize the impact of an attack and help the organization resist:

- **Switching from a fail-safe to safe-to-fail**

  Organizations have been right to focus so far on building robust, sturdy, resilient fail-safe operations that can withstand sudden cyber attacks. But in the face of today's unpredictable and unprecedented cyber threats, a fail-safe approach can no longer be the only option. The new aim should be to design a system that is safe-to-fail. Future cybersecurity needs to be smarter as well as stronger, with a soft-resilience approach. This means that on sensing a threat, there are mechanisms that have been designed to absorb the attack, reduce the velocity and impact of it, and accept the possibility of partial system failure as a way to limit damage to the whole.

- **From protection to sacrifice**

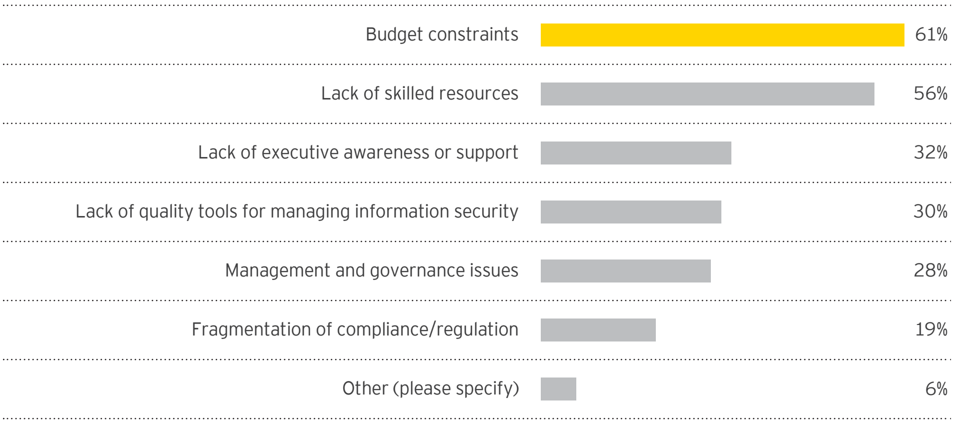
  Technologies today make it possible to sacrifice portions of information or operations in the interests of protecting the larger network. If configured correctly to the organization's risk appetite this can be performed as an automated response. When the SOC recognizes a high-level threat to the system, the system owner receives an alert and the system is shut down to prevent the spread of the threat.

Every year budgets increase, but is it enough?

Between 2013 and 2016 we have seen year on year increases in budgets, with 53% of responders this year saying their budgets increased over the last 12 months, compared with 43% in 2013, and 55% of responders today saying their budgets will increase over the coming 12 months, compared with 50% in 2013. The amounts being spent are also rising: in 2013, 76% of responders were spending less than $2m in total (which included people, process and technology); today only 64% are spending less than $2m and there has been a rise in the number of organizations spending between $10m–$50m.

Still, however, organizations say that more funding is needed, with 61% citing budget constraints as a challenge and 69% of responders saying they need up to 50% more budget. And it is not just budget that is needed. While additional budget may help alleviate the skills shortage, money cannot buy the executive support that is also needed.

What are the main obstacles or reasons that challenge your Information Security operation's contribution and value to the organization? (Select all that apply)



53%

of responders this year are saying their budgets increased over the last 12 months.

86%

of responders say they need up to 50% more budget.

89%

of organizations do not evaluate the financial impact of every significant breach.

The role of leadership

Executive leadership and support is critical for effective cyber resilience. Unlike the Sense and traditional Resist activities which can be seen as the domain of the CISO or CIO, cyber resilience requires senior executives to actively take part and lead the React phase. Since 2013 the survey has reported that 31%–32% of responders say there is a lack of executive awareness and support which is challenging the effectiveness of cybersecurity. This year on year consistency suggests not enough is being done to address this, or attempts have reached a deadlock and the message is not getting through.

The importance of reporting

Among our responders, 75% say that those responsible for information security do not have a seat on the board, so with this being the case, the board has to rely on reporting instead. Our survey revealed the following:

- Only 25% of reporting provides an overall threat level.
- Only 35% of reporting showed where improvements were needed in the organization's information security.
- Eighty nine percent of organizations do not evaluate the financial impact of every significant breach and of those that have had a cyber incident in the last year, nearly half (49%) have no idea what the financial damage is or could be.

With the quality of reporting being so low, it is no surprise that 52% of responders think their boards are not fully knowledgeable about the risks the organization is taking and the measures that are in place. In other words, our survey suggests that about half of all boards are flying blind in the face of the greatest threat to their organizations today.

49%

have no idea what the financial damage of a cyber attack is or could be.

React

Today's emergency services: the cyber breach response program

Given the likelihood that all businesses will eventually face a cyber breach, it is critical that companies develop a strong, centralized response framework as part of their overall enterprise risk management strategy.

A centralized, enterprise-wide cyber breach response program (CBRP) is the focal point that brings together the wide variety of stakeholders that must collaborate to resolve a breach. The CBRP should be led by someone who is experienced with technology, and is able to manage the day-to-day operational and tactical response, plus they must be equipped with in-depth legal and compliance experience, as these events can trigger complex legal and regulatory issues with financial statement impact.

The CBRP goes beyond the capacity of a traditional program management office. In its coordination and oversight role, the CBRP can help ensure that an organization's business continuity plan is appropriately implemented, that a communication and briefing plan among all internal stakeholders is developed and enforced, and that all breach-related inquiries received from external and internal groups are centrally managed. In short, the CBRP provides guidance to all lines of business involved in the response. The program sets a level of understanding about what information is critical for senior leaders to know — as well as when and how to express it, and allows continuous reaction with precision and speed as a breach continues to unfold over days, weeks or even months.

An effective CBRP must include the key constituencies in a high impact breach. Even as investigators need to work closely with information security and IT personnel to determine the attack vector, exploited networks and systems, and the scope of assets stolen or impacted, a CBRP is the linchpin of the response. The CBRP not only oversees the process of evidence identification, collection and preservation, forensic data analysis, and impact assessment, but also can direct and modify the investigation based on fact-pattern analysis.

The CBRP helps ensure the smooth and timely flow of information among the internal stakeholders and helps the organization navigate the complexities of working with outside legal counsel, regulators and law enforcement agencies. A robust CBRP, therefore, enables a cost-effective response that mitigates breach impacts by integrating the stakeholders and their knowledge.

What are the React priorities?

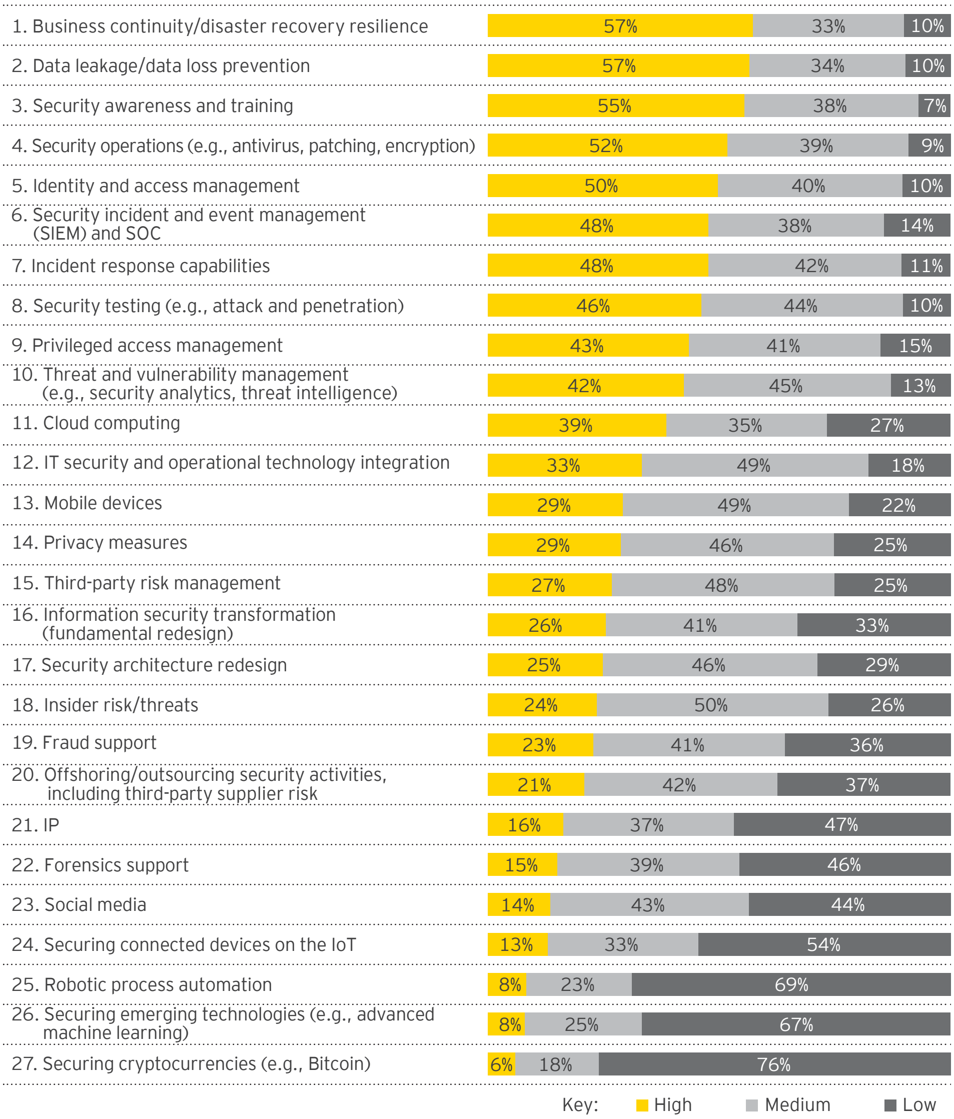
Business continuity management (BCM) has been at the heart of an organization's ability to react to a threat, attack or other disruption for many years. As a key area of cybersecurity it has been the number 1 or number 2 high priority in our survey since 2013, so the importance of having some React capabilities is understood. Again this year, 57% of organizations rated it their joint top priority, alongside data leakage/data loss prevention.

Security information and event management (SIEM) together with security operation centers (SOCs), ranked 6th, with 46% of the respondents saying that they are going to spend more in these two areas over the coming 12 months, ranking it second after security awareness and training.

57%

of organizations rated BCM as their joint top priority, alongside data leakage/data loss prevention.

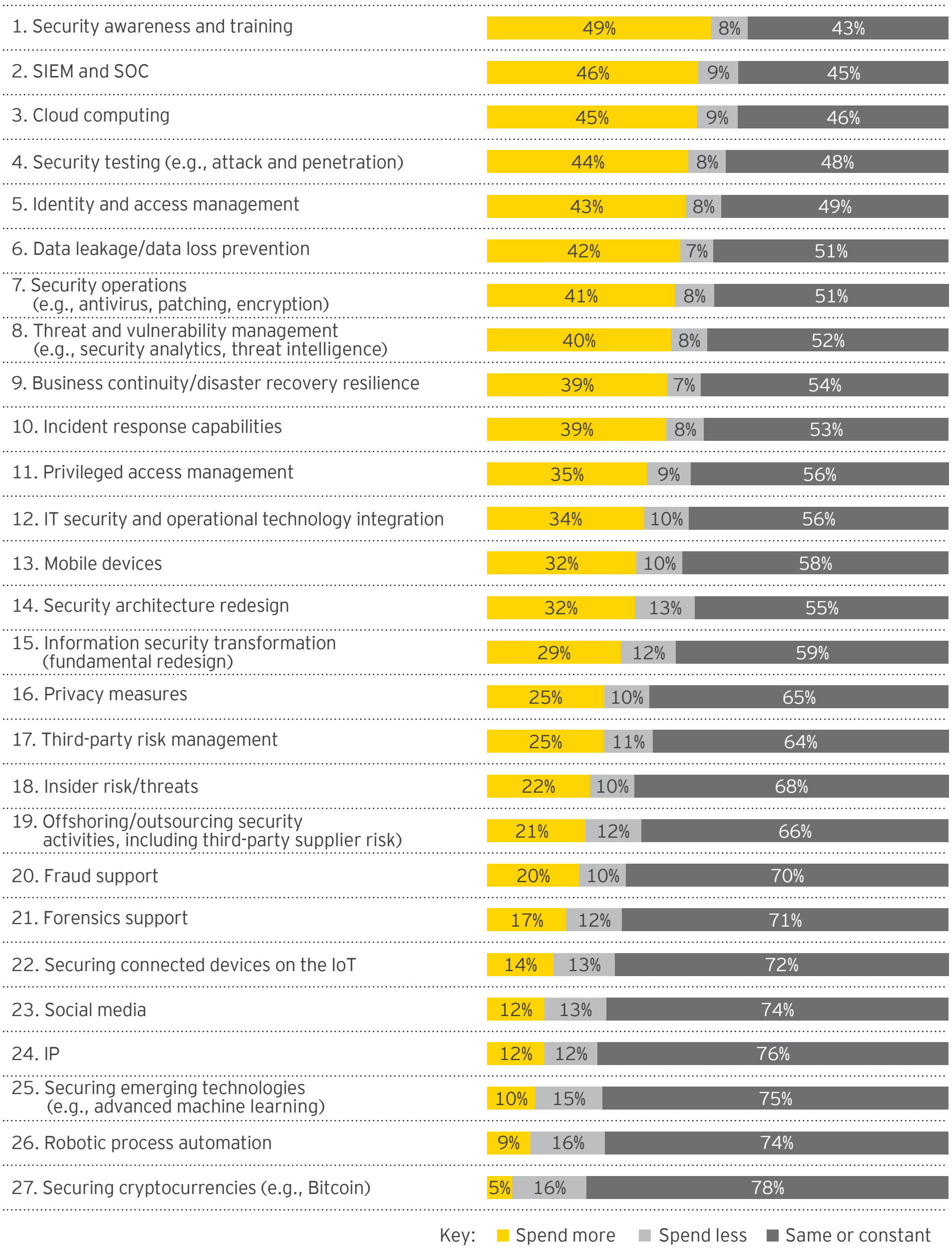
Which of the following information security areas would you define as "high, medium or low priorities" for your organization over the coming 12 months? (Select one response for each)



Where is the money spent?

Where organizations choose to put their budgets is a different picture. Looking at where organizations want to spend more, BCM ranks 9th. Organizations may feel that BCM has been well funded in the past and now they are investing in other React capabilities.

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the coming year for the following activities? (Select one response for each topic)



There is not a lot of appetite for investing in other adapt and reshape capabilities:

- **Adapt:** By looking at the threat horizon and threat actors, the resilient organization needs to be flexible and agile to adapt its business processes and protection mechanisms.
- **Reshape:** This is the re-engineering required to improve both the resilient and operational mechanisms for an increasingly secure and sustainable organization.

Despite outdated information security controls or architecture being the second highest vulnerability, 74% say that an information security transformation (fundamental redesign) is a medium or low priority, and 75% say a security architecture redesign is a medium or low priority.

When reacting to an attack, the board must show leadership

When it comes to immediately dealing with a cyber attack that has damaged the organization, there is nowhere today that the board can hide. If any weaknesses or failures in the recovery plans become known, and the longer these problems continue, the worse the situation will get. Some organizations may physically recover from an attack, but their reputation and trust can be destroyed. The key is to communicate and lead the communications before the strength of the traditional news media and social media takes over. Too many organizations are still unprepared.

- Forty two percent do not have an agreed communications strategy or plan in place in the event of a significant attack.
- In the first seven days after an attack:
  - Thirty nine percent say they would make a public statement to the media.
  - Seventy percent would notify regulators and compliance organizations.
  - Forty six percent would not notify customers, even when it is customer data that has been compromised.
  - Fifty six percent would not notify suppliers, even when it is supplier data that has been compromised.

42%

do not have an agreed communications strategy or plan in place in the event of a significant attack.

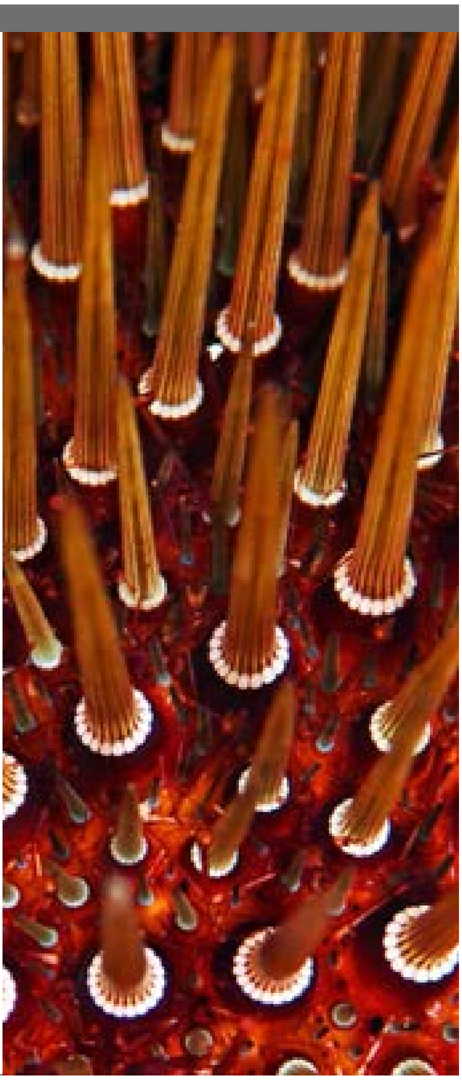
39%

say they would make a public statement to the media.

What, how and when to communicate can present significant challenges

- Today, many of the proposed regulations or laws around reporting of cyber attacks say that you need to notify customers within a certain number of days – 60 days, for example.* The problem there is that many cyber attacks are not discovered for months, sometimes years. And in cases where law enforcement is involved, they may request that you do not notify your customers while their investigations continue.
- Customers may be entitled, or feel entitled, to compensation for a breach of their information. In one example in the US, it is being discussed that a customer receives a year of free identity theft insurance. But not all breaches create a situation where a customer would need this, or something else like it, so there is a feeling that this kind of compensation would increase costs without actually providing a real benefit to the customer, and could be damaging to the brand and reputation.
- Finally, there is a growing recognition that it may be dangerous to notify customers every time, especially if the risk is low, as they can become desensitized and not respond when a more harmful incident occurs. If we think back over the last two years, it is not impossible that the same person has been notified about an attack on their mobile phone provider, the online retailer they use, their email provider, and they may have been advised their credit card details have possibly been sold and their social security records are perhaps in the hands of criminals, and there is nothing they can do about any of that. It is too much and people will start to ignore it.

* As in the case for the NAIC Roadmap for Cybersecurity Consumer Protections in the US



5%

of responders have recently made a significant change to their organization's strategy and plans.

Leading the recovery of the organization

For the CIO or CISO to be able to support the business during the adapting and reshaping phase, they need to fully understand the organization's strategic direction, risk appetite and operations. By bringing together the corporate strategists, and the corporate security team, the cybersecurity solution and the organization's overall strategy can be aligned. However, our survey shows that there is not a good connection between the cybersecurity function and the organization's strategy and planning.

- Only 5% of responders have recently made a significant change to their organization's strategy and plans, after sensing they were exposed to too much risk
- Only 22% say that they have fully considered the information security implications of their organization's current strategy and plans

79%

do their own self-phishing.

Asking tougher questions and closing the gaps

Our survey revealed how much organizations like to rely upon themselves to test or manage their own cybersecurity. In the recovery phase it may be worthwhile to consider whether this should continue. Currently, the following is true:

- Seventy nine percent do their own self-phishing.
- Sixty four percent do their own penetration testing.
- Eighty one percent do their own incident investigation.
- Eighty three percent do their own threat intelligence analysis.

Our survey also found gaps that need to be addressed. Despite careless employees, phishing and malware being such major and known threats, only 24% have an incident response plan that would help them recover from malware and employee misbehavior.

81%

do their own incident investigation.

Overall, considerable improvement still needed

Although React capabilities perform well in the priority ratings, the absolute amounts of money spent in this area are still relatively low. It became clear – from the overall state of cyber resilience (section 1) – that React is the area where most of the work is still to be done. The more it becomes clear that the corporate shield cannot resist all threats, the more attention the React capabilities will get.

Key characteristics of a cyber resilient enterprise

Understands the business

Cyber resilience demands a "whole of organization" response. It begins with an in-depth understanding of the business and operational landscape, to know which business workflows must be preserved so the organization can continue to operate and safeguard people, assets and overall brand equity, despite the cyber attack.

Understands the cyber ecosystem

Map and assess the relationships the organization has across the cyber ecosystem and identify what risks exist. Perform a risk assessment of the organization's cyber presence in the ecosystem, determining those factors that affect the extent of the organization's control over its ecosystem.

Determines the critical assets — the crown jewels

Most organizations over-protect some assets and under-protect others. In the survey:

- Fifty one percent ranked customer personal identifiable information as the number 1 or number 2 information most valuable to cybercriminals in the organization.
- Only 11% rated patented IP the number 1 or number 2 most valuable information.
- Senior executive/board member personal information was considered more valuable than R&D information, patented IP and non-patented IP, and broadly on a par with corporate strategic plans.

Determines the risk factors

Cybersecurity functions can only achieve limited success with a limited view of the risk and threat landscape. Over and above all of the technologies and tools that can provide better awareness, intelligence and identification of threats, is the concept of collaboration. Sharing information about the risk and threat landscape of all the business functions allows the organization to understand their broader risk landscape and expose any security gaps. This sharing and collaboration can then extend to other organizations (partners, suppliers) in the same ecosystem.

Organizations then need to ask the following:

- How much can we do to manage any residual risk?
- Are we prepared to accept a certain level of risk?
- What can we attempt to control and what do we need to accept is out of our control?

Manages the human element with exceptional leadership

After a cyber attack, as in any chaotic situation, individuals need to be prepared and trained on how to respond and behave. With technology supporting the entire organization, every employee will be impacted. Clear communication, direction and example-setting from leadership will be essential, as well as clearly defined roles or tasks that they are able to perform to help the organization become operational again.

Creates a culture of change readiness

The capability to react rapidly to a cyber attack will minimize the possibility of long-term material impacts. Organizations that develop superior, integrated and automated response capabilities can activate non-routine leadership, crisis management and coordination of enterprise-wide resources. As a simulation exercise, organizations can challenge the existing crisis management, current practices and risk profile to make sure they are fully aligned with the organization's business strategy and risk appetite.

Organizations should also develop and implement tailor-made war games that would include a review of any command and control center, cyber resilience manuals and plans.

Conducts formal investigations and prepares for prosecution

To protect the interests of the organization in the event of a major cyber-breach, the CIO and CISO should be prepared to liaise with the most senior executives from Security, General Counsel, External Counsel, Investigations and Compliance. Together they will:

- Collect evidence in a forensically sound way, in order to support a wider investigation.
- Establish whether the attackers still have footholds in the organization's networks and systems, and whether harmful malware or ransom-ware could sabotage the organization again in future.
- Perform deeper investigations to understand who carried out the attack, how they performed it, for whom and why.
- Be able to bring a claim against either the attacker, and/or criminal prosecution, as well as those who aided and abetted the attacker, or otherwise enabled the attack. Claims can also be brought against product and service providers who failed to meet contractual obligations to build, operate, test or maintain cybersecurity.

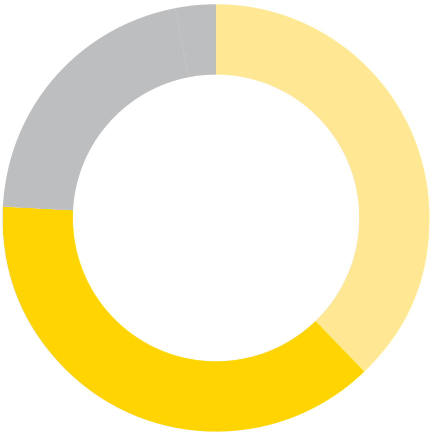
Survey methodology

EY's 19th *Global Information Security Survey* captures the responses of 1,735 C-suite leaders and Information Security and IT executives/managers, representing many of the world's largest and most recognized global companies. The research was conducted between June–August 2016.

Respondents by position

Chief Information Security Officer	23%
Information Security Executive	12%
Chief Information Officer	12%
Information Technology Executive	11%
Chief Security Officer	3%
Internal Audit Director/manager	3%
Chief Technology Officer	3%
Network/System Administrator	2%
Business Unit Executive/ Vice President	2%
Chief Financial Officer	1%
Chief Risk Officer	1%
Other	27%

Respondents by area



Key:

▨	EMEIA	38%
■	Americas	38%
▨	Asia-Pacific and Japan	24%

Respondents by number of employees

Less than 1,000	34%
1,000 to 1,999	14%
2,000 to 2,999	7%
3,000 to 3,999	5%
4,000 to 4,999	4%
5,000 to 7,499	7%
7,500 to 9,999	6%
10,000 to 14,999	6%
15,000 to 19,999	4%
20,000 to 29,999	3%
30,000 to 39,999	3%
40,000 to 49,999	2%
50,000 to 74,999	2%
75,000 to 99,999	1%
100,000 and above	4%

Respondents by total annual company revenue

Less than **US$10m**	7%
US$10m to less than **US$25m**	4%
US$25m to less than **US$50m**	5%
US$50m to less than **US$100m**	4%
US$100m to less than **US$250m**	9%
US$250m to less than **US$500m**	9%
US$500m to less than **US$1b**	10%
US$1b to less than **US$2b**	9%
US$2b to less than **US$3b**	5%
US$3b to less than **US$4b**	3%
US$4b to less than **US$5b**	2%
US$5b to less than **US$7.5b**	3%
US$7.5b to less than **US$10b**	3%
US$10b to less than **US$15b**	5%
US$15b to less than **US$20b**	2%
US$20b to less than **US$50b**	3%
US$50b or more	3%
Government, non-profit	7%
Not applicable	7%

Respondents by industry sector

Banking & Capital Markets	20%
Insurance	7%
Technology	7%
Consumer Products	6%
Government & Public Sector	6%
Diversified Industrial Products	5%
Power & Utilities	5%
Retail & Wholesale	4%
Telecommunications	4%
Health care	4%
Media & Entertainment	3%
Professional Firms & Services	3%
Real Estate (including Construction, Hospitality & Leisure)	3%
Oil & Gas	3%
Automotive	3%
Transportation	2%
Mining & Metals	2%
Wealth & Asset Management	2%
Life Sciences	2%
Airlines	1%
Chemicals	1%
Aerospace & Defense	1%
Other	6%

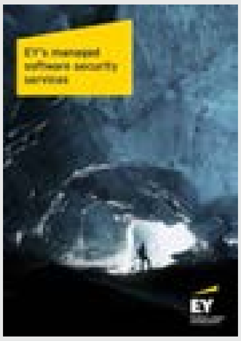
Want to learn more?

Our cybersecurity publications and thought leadership reports are designed to help you understand the issues and provide you with valuable insights about our perspectives. Please visit our Insights on governance, risk and compliance series at ey.com/GRCinsights and our website ey.com/cybersecurity.

How do you find the criminals before they commit the cybercrime?
EY

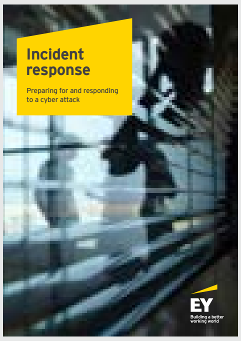
How do you find the criminals before they commit the cybercrime?: a closer look at cyber threat intelligence

ey.com/cti



Managed software security services: building a software security center of excellence

ey.com/GRCinsights


Incident response
Preparing for and responding to a cyber attack
EY
Building a better working world

Incident response

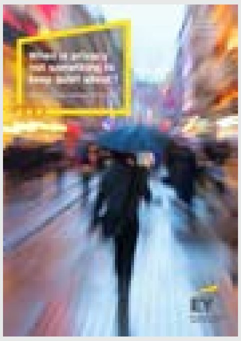
ey.com/GRCinsights

Managed SOC: EY's Advanced Security Center

ey.com/soc

Using cyber analytics to help you get on top of cybercrime: third-generation Security Operations Centers

ey.com/soc



When is privacy not something to keep quiet about?: the EU General Data Protection Regulation

ey.com/GRCinsights

Privacy trends 2016: can privacy really be protected anymore?

ey.com/privacytrends

Active Defense

ey.com/activedefense

Creating trust in the digital world: EY's Global Information Security Survey 2015

ey.com/giss2015

If you were under cyber attack, would you ever know?

For EY Advisory, a better working world means solving big, complex industry issues and capitalizing on opportunities to help provide outcomes that grow, optimize and protect our clients' businesses. We've shaped a global ecosystem of consultants, industry professionals and business alliances with one focus in mind — you.

We believe anticipating, and now actively defending against, cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then work with you to create more innovative answers that help provide the approaches you need. Together, we help you achieve better outcomes and long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.

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

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.

EYG no. 04260-163GBL

BMC Agency

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.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/giss

About EY's Advisory Services

In a world of unprecedented change, 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.

From C-suite and functional leaders of Fortune 100 multinationals to disruptive innovators and emerging market small- and medium-sized enterprises, EY Advisory works with clients — from strategy through execution — to help them design better outcomes and realize long-lasting results.

A global mindset, diversity and collaborative culture inspires EY consultants to ask better questions. They work with their clients, as well as an ecosystem of internal and external experts, to create innovative answers. Together, EY helps clients' businesses work better.

For questions about cybersecurity, please contact our cybersecurity leaders:

Global		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
David Remnitz	+1 212 773 1311	david.remnitz@ey.com
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
Timothy Ryan	+1 212 773 0410	timothy.ryan@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Paul Walker	+44 207 951 6935	pwalker@uk.ey.com
Asia-Pacific		
Richard Watson	+61 2 9276 9926	richard.watson@au.ey.com
Reuben Khoo	+65 6309 8099	reuben.khoo@sg.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 3500	azuma-yshhr@shinnihon.or.jp
Ichiro Sugiyama	+81 3 3503 3500	sugiyama-chr@shinnihon.or.jp