

An owl with large yellow eyes and brown feathers is peering through a hole in a tree trunk. The owl's face is the central focus, with its eyes looking directly at the viewer. The tree bark is rough and textured, and the lighting is natural, highlighting the owl's features.

Cybersecurity regained: preparing to face cyber attacks

20th Global Information Security Survey
2017-18

Contents

Welcome	01
Section 1: Confront your cyber threats	02
Section 2: Understanding the threat landscape	06
Section 3: Fighting back against the threat	10
Section 4: Emergency service: responding to an attack	18
Section 5: Conclusion	22
Section 5: Survey methodology	26





Paul van Kessel
EY Global Advisory
Cybersecurity Leader

Welcome

Welcome to the 20th EY Global Information Security Survey (GISS) exploring the most important cybersecurity issues facing organizations today.

Two decades after EY first began publishing annual surveys detailing organizations' concerns about cybersecurity – and their efforts to confront these concerns – the imperative for a collaborative and coherent response to the changed threats could hardly be more pressing. In our conversations with organizations of all shapes and sizes, it is clear cybersecurity is a priority issue from board level down. But in a complex and evolving landscape, it can be difficult to see the wood for the trees: the cybersecurity threat is often well-camouflaged, hidden in plain sight.

This year, we are delighted that nearly 1,200 organizations were able to participate in the survey. We have analyzed the responses of the CIOs, CISOs and other executives of these organizations, identifying strengths and weaknesses with the aim of generating insight from which we can all benefit. The GISS-report also draws on our own extensive experience of working with clients globally to improve their cybersecurity resilience.

If your organization is feeling anxious about cybersecurity, it may be some comfort to know that you are not alone: most organizations feel they are more at risk today than 12 months ago. No wonder: not only are cyber attackers becoming more sophisticated, but also, organizations themselves are increasingly hyper-connected with wave upon wave of new technology creating opportunities and risks across the value chain. This explosion of connectivity fueled by the growth of the Internet of Things (IoT) and the ever-larger digital footprint of many organizations have all introduced new vulnerabilities for attackers to exploit. It's why businesses need to explore digital from every angle to help them grow and protect their organizations today, tomorrow and far into the future.

However, despite the risks, there is good news too. Organizations that confront the cybersecurity challenge will regain a sense of order: it is not possible to repel every threat, but resilient organizations know how to protect themselves, how to detect a problem when it occurs, and how to react quickly and effectively when trouble strikes.

Moreover, we now have a good understanding of the most common attack methods and an appreciation of the ingredients of good cybersecurity hygiene, with which most such attacks can be defeated. Active defense strategies and advanced threat intelligence provide a basis for withstanding more advanced attack methods, and while new attack methods are emerging all the time, good cybersecurity governance and concepts such as security-by-design give organizations a fighting chance.

Working together, we can regain cybersecurity. With that in mind, we would like to thank clients for taking the time to complete the survey: let us continue to share our knowledge in order to build a safer world for us all.

Section

1



Confront your cyber threats

Nowadays, all organizations are digital by default. Not every organization delivers its products and services primarily through digital channels, but all operate with the cultures, technology and processes of the internet era. Moreover, in the connected and convergent world delivered by the Internet of Things (IoT), the digital landscape is vast, with every asset owned or used by the organization representing another node in the network.

No wonder the World Economic Forum now rates a large-scale breach of cybersecurity as one of the five most serious risks facing the world today.¹ The scale of the threat is expanding drastically: by 2021, the global cost of cybersecurity breaches will reach US\$6 trillion by some estimates, double the total for 2015.²

Cyber attackers can be either indiscriminate or highly targeted, attacking large and small organizations in both the public and private sector. They are well camouflaged: exposing the attackers requires cybersecurity defenses that identify the threat, even when it adopts the colors of its immediate environment. Organizations do not always manage this.

This year alone, in the UK the ransomware attack WannaCry affected a significant part of the National Health Service (NHS);³ in France, a breach of the Presidential campaign of Emmanuel Macron threatened to throw the election into chaos;⁴ in the US, Yahoo disclosed that a breach saw 3 billion user accounts compromised,⁵ while in India an attack paralyzed the biggest container port in Mumbai.⁶

At the same time, it has never been more difficult for organizations to map the digital environment in which they operate, or their interactions with it. Every organization's technology infrastructure is both bespoke and complex, spanning networks consisting of tools and technologies that may be on-premises or in the cloud. In addition, it is becoming more difficult to define an "organization." This is due to the proliferation of devices belonging to employees, customers and suppliers (including laptops, tablets, mobile phones and more) with access to the organization's systems that blur the security perimeter. Organizations must think of themselves as having long and trailing tentacles in every direction.

¹ "Global Risks Report 2017", *World Economic Forum*, 11 January 2017.

² "Cybercrime Report 2017 Edition", *Cybersecurity Ventures*, 19 October 2017.

³ "Investigation: WannaCry cyber attack and the NHS", *National Audit Office*, 27 October 2017.

⁴ "Hackers hit Macron campaign with 'massive' attack," *Financial Times*, 6 May 2017.

⁵ "All 3 billion Yahoo Accounts Were Affected by 2013 Attack," *The New York Times*, 3 October 2017.

⁶ "Petya cyber attack: India is worst affected in Asia, Ukraine on top globally," *The Indian Express*, 29 June 2017.

Connected devices add to the complexity. The IoT is not a collection of passive items; rather it is network of connected and inter-connected devices that actively and constantly interact. The convergence of these networks with what were once separate and self-contained – and therefore more manageable – systems represents fundamental change.

The stakes could hardly be higher. Organizations that fall prey to a cyber attack are at risk of substantial reputational loss as well as the direct costs of a breach, estimated to average US\$3.62m by the Ponemon Institute.⁷ There is also the potential for damaging confrontations with authorities and regulators. The European Union's General Data Protection Regulation (GDPR), due to come into force in 2018, gives regulators powers to fine organizations up to 2% of their global annual turnover for failures relating to a breach, and 4% if an organization significantly mismanages a response.⁸

Nor is it only data and privacy that are vulnerable. The IoT exposes organizations' operational technologies to attackers, offering them an opportunity to shut down or subvert industrial controls systems, for example. The threat may even be to life: imagine the attacker with the ability to turn off life support systems in hospitals or take control of connected cars on the road.

Mounting threat levels require a more robust response and this year's GISS reveals that many organizations continue to increase their spending on cybersecurity. Seventy percent say they require up to 25% more funding, and the rest require even more than this. However, only 12% expect to receive an increase of more than 25%.



59%

of respondents this year say their budgets increased over the last 12 months.



87%

say they need up to 50% more budget.



12%

expect an increase of more than 25% in their cybersecurity budget.

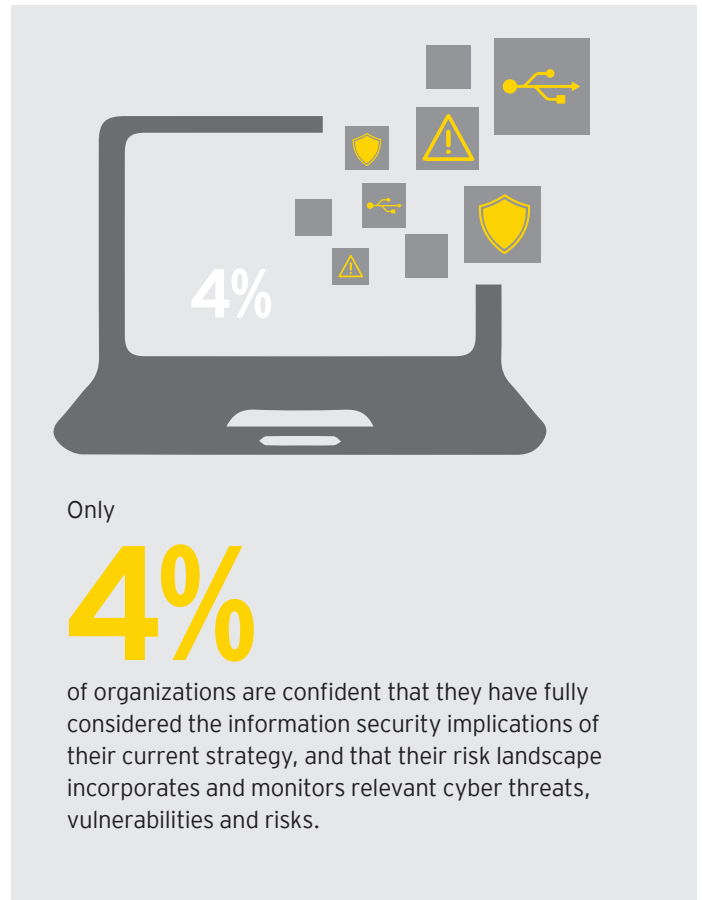
⁷ "2017 Cost of Data Breach Study", *The Ponemon Institute*, June 2017.

⁸ "GDPR Portal: Site Overview", *European Union*, October 2017.

For many organizations, the worst may have to happen for these calls to be met. Asked what kind of event would result in cybersecurity budgets being increased, 76% of survey respondents said the discovery of a breach that caused damage would be likely to see greater resources allocated.

By contrast, 64% said an attack that did not appear to have caused any harm would be unlikely to prompt an increase in the organization's cybersecurity budget. This is higher than the figure reported last year, which is concerning given the reality that harm is generally being done by an attack even it is not immediately obvious. The breach may be a test attack that exposes vulnerability or a diversion designed to take attention away from another more damaging threat; alternatively, the attacker may simply be biding their time before capitalizing on the breach. Organizations should assume all attacks are harmful and conclude that where harm has not been identified, this is only because it has not yet been discovered.

Ultimately, organizations that fail to devote the resources necessary for adequate cybersecurity will find it very difficult to manage the risks they face. Our survey suggests organizations increasingly recognize this: 56% of respondents say either that they have made changes to their strategies and plans to take account of the risks posed by cyber threats, or that they are about to review strategy in this context. However, only 4% of organizations are confident they have fully considered the information security implications of their current strategy and incorporated all relevant risks and threats.



Section

2



Understanding the threat landscape

The first step for organizations seeking to enhance their cybersecurity ability is to develop a better understanding of the nature of the threat to them. It will not be possible to build greater cybersecurity resilience into the organization without first identifying the potential causes of harm and how they might manifest themselves. Situational awareness is crucial – what are the threats and what do they mean for you and your organization?

Moreover, the range of potential attacks – and attackers – is wide and becoming more so by the day. Organizations may feel more confident about confronting the types of attack that have become familiar in recent years, but still lack the capability to deal with more advanced, targeted assaults; they may not even be aware of attack methods that are emerging. To be cyber resilient, however, organizations must increase their understanding rapidly – it is likely that they will face all of these categories of attack at one time or another, and possibly simultaneously.

The threat landscape

	Common attacks	Advanced attacks	Emerging attacks
What is it?	These are attacks that exploit known vulnerabilities using freely available hacking tools, with little expertise required to be successful	Advanced attacks exploit complex and sometimes unknown (“zero-day”) vulnerabilities using sophisticated tools and methodologies	These attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, based on specific research to identify and exploit vulnerabilities
Typical threat actors	Unsophisticated attackers, such as disgruntled insiders, business competitors, hacktivists and some organized crime groups	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states	Sophisticated attackers such as organized crime groups, industrial espionage teams, cyber terrorists and nation states
Examples	<ul style="list-style-type: none"> ▶ Unpatched vulnerability on a website, exploited using a freely available exploit kit ▶ Generic malware delivered through a phishing campaign, enabling remote access to an endpoint ▶ Distributed Denial of Service (DDoS) attack for hire with a basic random demand 	<ul style="list-style-type: none"> ▶ Spear phishing attacks using custom malware ▶ “Zero-day” vulnerabilities exploited using custom-built exploit code ▶ Rogue employees “planted” to undertake deep reconnaissance/espionage ▶ Vendors/suppliers exploited as a way to gain access to ultimate target organization 	<ul style="list-style-type: none"> ▶ Exploiting vulnerabilities on “smart” devices to gain access to data and/or control systems ▶ Leveraging security gaps created with the convergence of personal and corporate devices into one network ▶ Using advanced techniques to avoid detection and/or bypass defenses

All organizations must assume that the worst could happen – there is no excuse for assuming otherwise. There have been too many well-known and worldwide attacks for complacency to be acceptable.

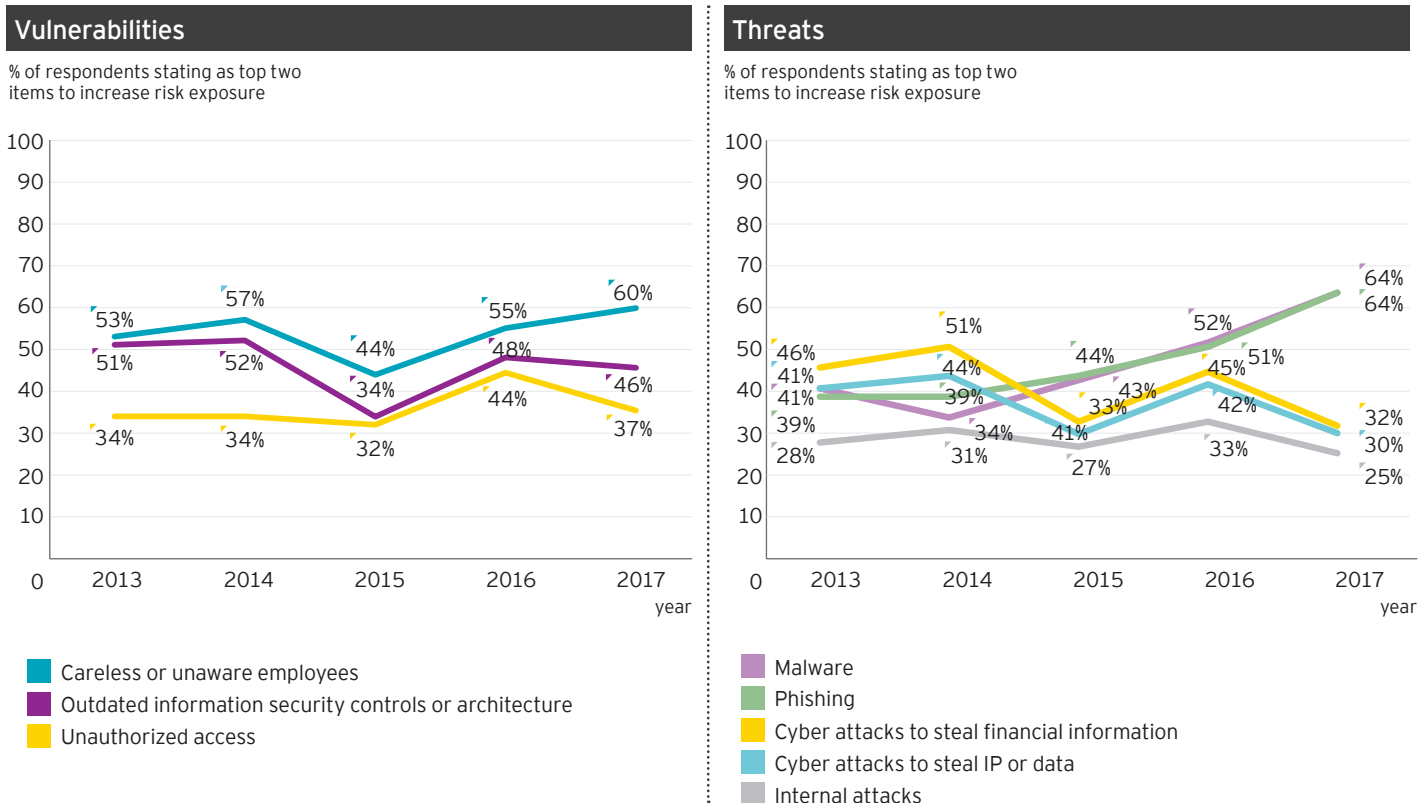
Take the Petya ransomware attack that so badly affected organizations around the world in late June of 2017, affecting tens of thousands of public and private sector enterprises. The vendor had previously released a patch for the exploited weakness – organizations that did not apply this update, perhaps because they did not understand the threat to them, were left wide open to the attack.

The Mirai attack, by contrast, is more sophisticated and underlines the broader vulnerabilities that organizations must understand and address. One such attack on the Dyn DNS provider last year brought much of the internet to a standstill, disrupting organizations including Twitter and Spotify⁹ amongst

others. In that attack, Mirai targeted unprotected webcams, but it has also used CCTV camera networks, and in theory could target any “smart” – that is internet-connected – device. In this case, failure to understand or anticipate the threat left organizations complacent about ensuring that factory-setting passwords on all network-connected smart devices had been updated.

With so many disparate threats – and perpetrators that could be anyone from a rogue employer to a terrorist group or a nation state – organizations must be vigilant across the board and be well acquainted with their own threat landscape. All the more so since attackers have easy access to malware and sophisticated tools – and can even hire cyber-criminals – online.

Threats and vulnerabilities perceived to have most increased the risk exposure of the respondents, 2013-2017



⁹“Internet outage takes down Twitter, Netflix, Paypal and many more of the web’s most visited websites,” *The Independent*, 21 October 2016.

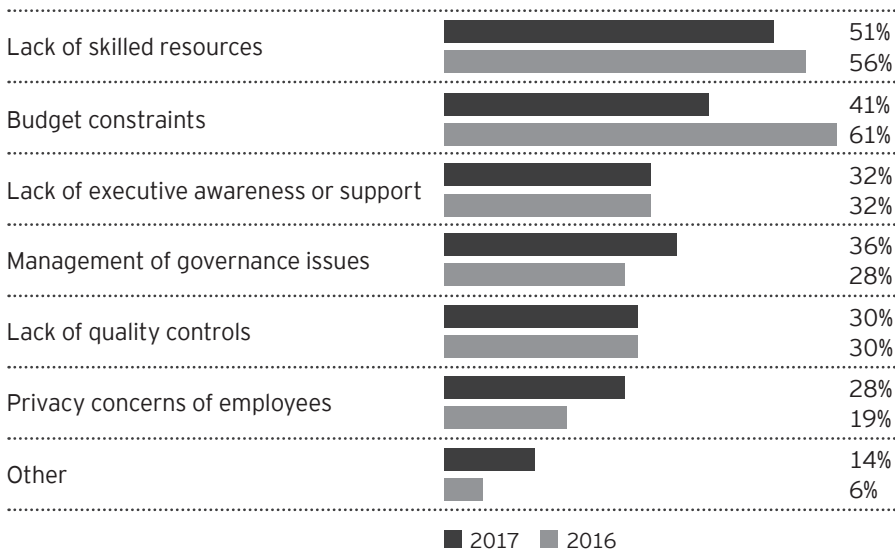
The previous chart shows how careless or unaware employees are still seen as an increasing risk, while interestingly unauthorized access has greatly reduced as a perceived risk.

Employees and criminal syndicates are seen as the greatest immediate threats. For many organizations, the most obvious point of weakness will come from an employee who is careless or fails to heed the cybersecurity guidelines.

Organizations are also increasingly fearful about the vulnerabilities within new channels and tools. For example, 77% of survey respondents worry about poor user awareness and behavior exposing them to risk via a mobile device; the loss of such a device, and the potential for loss of information and an identity breach, are a concern for 50%.

The IoT meanwhile is the source of a broad range of threats that many organizations are now struggling to better understand. The next chart outlines some of the issues around IoT integration.

Obstacles slowing down adoption of IoT devices (multiple answers possible)



Understand the problem to address the right challenge

The story of St. Helena provides a neat metaphor for where some organizations are still going wrong with their cybersecurity efforts. A remote island in the South Atlantic Ocean, St. Helena has long been accessible only by long and difficult sea journeys, so its inhabitants were delighted when a US\$370m project to build a landing strip was completed in 2016. Sadly, commercial airlines initially refused to use the runway, which has been built on the edge of a near-vertical 1,000 foot cliff, between two rocky outcrops that funnel a fierce wind. Pilots warned it was too dangerous to attempt a safe landing.

The problem here is that those behind the project focused on the wrong problem: the lack of a runway on the island. What they should have thought about was the lack of a safe place to land a plane.

The read-across to cybersecurity is that while all organizations discuss cybersecurity in their boardrooms, often making huge investments, it is not always clear which problem they're solving. Are they focused on just adding more cybersecurity technology or on solving the lack of cyber resilience?

Clearly, the latter should be the target, but to get there, the organization needs to understand the relationship between cyber resilience and the objectives of the business, as well as the nature of the risks it is facing and the status of the current safeguards. It must also assess how much risk it is prepared to take, and define an acceptable loss. Only when these steps have been taken can the organization make targeted and cost-effective investments in cybersecurity.

Fortunately, commercial flights commenced in St. Helena during October 2017, and we are also seeing more boards discussing and understanding their cyber risks and desired cyber resiliency before allocating the cybersecurity budget.

Section

3



Fighting back against the threat

Organizations are likely to be confronted by a wave of attackers of varying levels of sophistication, and they can and must fight back. The response must be multilayered: focused on repelling the most common attacks/threats that the organization is more confident of defending against, but also conscious that a more nuanced approach is necessary for dealing with advanced and emerging types of attack. As some of these attacks will inevitably breach the organization's defenses, the focus needs to be on how quickly they are detected, and how effectively they are dealt with.

Defending against the common attack methods

Organizations should think in terms of closing the door to the most common types of attack. According to Greg Young, Research Vice President at Gartner: "Through 2020, 99% of vulnerabilities exploited will continue to be the ones known by security and IT professionals for at least one year."¹⁰ Identifying and closing off these vulnerabilities in your organization before they are exploited is therefore crucial. Indeed with good cybersecurity hygiene in place – even if this is easier said than done – it should be possible to prevent a very sizeable proportion of common attacks. For the next few years, patching known vulnerabilities and removing web server vulnerabilities could be the most impactful actions for boosting your cybersecurity.

At this threat level, point solutions remain a key element of cybersecurity resilience, with tools including antivirus software, intruder detection and protection systems (IDS and IPS), consistent patch management and encryption technologies that protect the integrity of the data even if an attacker does gain access to it. Employee awareness is also a crucial frontline defense, building cybersecurity consciousness and password discipline throughout the organization. As the respondents to this survey point out, careless employee behaviors represent a significant point of weakness for most organizations; addressing this weakness is vital.

The maturity of an organization's cybersecurity approach will determine its effectiveness. In this year's survey, of all the cybersecurity management processes discussed, three areas correlated especially closely with the confidence of organizations in detecting a cyber attack: privacy, security monitoring and third-party management.

However, many organizations have serious concerns about the current maturity of their cybersecurity systems.

In order to defend against common threats organizations need to make sure that the basics are in place. The basics consist of five strategic components:

1. Talent-centric

Cybersecurity is not the sole responsibility of the IT department; it is the responsibility of every employee and even of all the people in the eco system of the organization.

2. Strategic and innovative

3. Risk focused

4. Intelligent and agile

5. Resilient and scalable



75%

of respondents rate the maturity of their vulnerability identification as very low to moderate.



35%

describe their data protection policies as ad-hoc or non-existent.



12%

have no breach detection program in place.



38%

have no identity and access program or have not formally agreed such a program.

¹⁰ "How to Address Threats in Today's Security Landscape", <https://www.gartner.com/smarterwithgartner/how-to-address-threats-in-todays-security-landscape/>, Gartner, 9 May 2017.



Ingredients required to achieve cybersecurity resilience

The pace of change in today's increasingly digitized world has led to the convergence of different risk disciplines that complement each other to address our clients' needs and those of their customers, regulators and business partners.

Putting cybersecurity at the heart of an organization's strategy will help maintain and even enhance the trust of consumers, regulators and the media. For a start, the C-suite can no longer assume that cybersecurity is solely the responsibility of the information security (IS) or information technology (IT) departments. Instead, organizations must make cybersecurity a core part of business strategy and culture. In doing so, they can enable the entire organization to understand the risks they face, embrace the innovation needed to counter those risks, and have the resilience to regroup and restore operations smoothly and efficiently in the wake of a cyber breach.

Organizations need an integrated cybersecurity vision – one that brings together the various functions and dependencies with other parts of the organization, external key stakeholders and third-party suppliers.



Defending against advanced attacks

If organizations are ambitious enough to seek to close the door on common types of cyber attack, they must also be realistic enough to accept that advanced attackers will get in. In which case it is crucial to be able to identify intrusions as quickly as possible – and to have processes that are known to provide the organization with an effective means to deal with the after-breach situation and to kick attackers back out.

A Security Operations Center (SOC) that sits at the heart of the organization's cyber threat detection capability is an excellent starting point, providing a centralized, structured and coordinating hub for all cybersecurity activities. SOCs are becoming increasingly common, but 48% of respondents still do not have one.

This does not mean the SOC has to build capability for every possible aspect of cybersecurity strategy and leading practice. Many organizations choose to outsource some activities, rather than leaving them with the in-house SOC; 41% of survey respondents outsource penetration testing, for example, while 37% outsource real-time network monitoring.

However, the SOC must have the means to ensure it is able to stay on top of the latest threats: open-source and paid-for resources may provide valuable intelligence and 36% of survey respondents point out their SOC collaborates and shares data with industry peers.

Moreover, SOCs are increasingly moving beyond passive cybersecurity practices into active defense – a deliberately planned and continuously executed campaign that aims to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization's most critical assets. Active defense represents a crucial step forward as organizations seek to counter advanced attackers, and can be thought of as a strategy encompassing at least four stages:

1 Prioritizing the crown jewels

In any organization, certain assets, including people, are particularly valuable and must be identified and then protected especially well; these assets may be related to critical business functions or particularly sensitive data repositories.

2 Defining normal

Since active defense depends on tools such as anomaly analysis, it is important for organizations to understand how their networks normally operate. Cybersecurity analytics tools use machine learning to define the "normal" and artificial intelligence to recognize potential malicious activity more quickly and accurately.

3 Advanced threat intelligence

By working closely with threat intelligence providers and developing in-house analyst capability, it is possible for organizations to build a much clearer picture of the threat landscape – including the identities of C-level executives. Currently, however, 57% have very little threat intelligence.

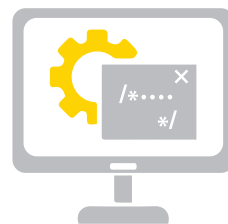
4 Active defense missions

These are exercises planned and executed in order to proactively defeat specific threat scenarios and uncover hidden intruders in the network. It requires tailored training and testing – spear phishing tests, for example, that identify how vulnerable employees are to email scams, penetration tests that pinpoint network vulnerabilities, and even full-blown red team testing.



48%

of respondents do not have a SOC.



57%

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

Employing these strategies can boost the organization's cyber resilience and also reduce its "dwell time" – the amount of time that an attacker can remain in the system undetected. This is crucial: only 12% of survey respondents say they would be very likely to detect a sophisticated cyber attack targeted at their organization. Amongst organizations that have experienced a cybersecurity incident, almost a third say the problem was uncovered by their SOC.



12%

feel it is very likely they would detect a sophisticated cyber attack.

Don't be dumb about smart buildings

Organizations' buildings increasingly represent a major cybersecurity vulnerability: the IoT and advances in operational technologies may underpin a new generation of "smart" buildings, but they also offer cyber attackers an enticing new entry point.

The nature of the threat is wide-ranging. Attackers may target the control systems of the building itself, jeopardizing safety with attacks on, say, fire protection systems or the elevator controls; even a brief shut-down of the building's air conditioning system could cause a crash in a data center. Alternatively, attackers may target the building's connected systems as a way into an organization's broader enterprise systems, piggy-backing on remote links and inter-connectivity.

The scope for damage from such attacks is huge. It ranges from the potential for disruption from system outages to a full-scale data breach enabled by a smart-building vulnerability. Ransomware may render a building unusable for a period. Organizations in regulated industries, including financial services, health and the public sector, may be exposed to sanctions from the relevant authorities. Reputational damage is very likely. The legal liabilities of building owners to their tenants in such events have yet to be fully explored. In a building such as a hospital, people's lives could even be in danger.

Despite these risks, however, many organizations are only just beginning to get to grips with the cybersecurity implications of their physical estate. Doing so is not straightforward: many of the operational technologies installed in business sit outside the IT function, where cybersecurity is more likely to be front of mind; connections have often been added piecemeal over many years, adding internet functionality to historic systems bit by bit, with no single function or individual maintaining an overview of the entire building; and much of the connectivity added in years gone by will have had little or no security built in.

Smart buildings, in other words, are not so smart from a cybersecurity perspective. The latest technologies, from smart lighting systems to garage parking controls, may be designed and installed with cybersecurity in mind, but they are being added to already-vulnerable systems.

Organizations must now get to grips with this risk, identifying their most critical buildings – where their most valuable assets reside, perhaps, or their most business-critical systems – and working quickly to map connectivity in order to assess cybersecurity and mitigate the risk with appropriate defenses. Once these priority buildings have been protected, this approach must be rolled out to the rest of the estate.

Defending against emerging attacks

In practice, no organization can anticipate all the threats that are emerging – the nature of such threats is that they will often be unknown, in which case the door may be wide open to the perpetrators of such attacks. However, innovative organizations able to be imaginative about the nature of potential future threats can build agility into their cybersecurity so that they are able to move fast when the time comes. Moreover, organizations with good governance processes underlying their operational approach are able to practice security-by-design – building systems and processes able to respond to unexpected risks and emerging dangers.

The study shows that cybersecurity budgets are higher in organizations that:

- ▶ Place dedicated business line security officers in key lines of business
- ▶ Report at least twice a year on cybersecurity to the board and audit committee
- ▶ Specifically identify non-IT crown jewels and differentially protect such assets



63%

of organizations still have the cybersecurity function reporting into IT.



89%

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



only

50%

report to Board regularly.



24%

say the person with responsibility for cybersecurity sits on their board.

To improve their chances of fighting back against cyber attackers, organizations will have to overcome the barriers currently making it more difficult for cybersecurity operations to add value. For example, 59% of respondents cite budget constraints while 58% lament a lack of skilled resources; 29% complain about a lack of executive awareness or support.



36%

of Boards have sufficient knowledge of information security to fully evaluate the effectiveness of the risks the organisation is facing and the measures the organisation is taking.

Cybersecurity for road safety

The connected car is already a reality. The automotive sector's steady progression toward increasingly autonomous vehicles depends on operational technologies that provide remote access to vehicle systems ranging from navigation to basic safety controls. Moreover, leading manufacturers now see software-over-the-air technology as the default option for maintaining, repairing and upgrading vehicles already sold to drivers. Those updates will span every aspect of the vehicle, from infotainment to telematics to control units.

Against this backdrop – a rapid shift from closed to open networks governing vehicle behavior and performance – cybersecurity is a crucial consideration. The risks posed by cyber attackers able to take control of a vehicle through poorly protected connectivity could hardly be more serious. An attacker has the ability to put the lives of the inhabitants of the vehicle, and other road users, at risk – even to weaponize the vehicle in order to deliberately target others.

Yet connected care technologies, like many other aspects of operational technologies and IoT applications, are being developed. The maturity of taking cyber risks and their mitigation into account is growing. The innovators who have done such good work across so many areas of automotive technology need to further increase their practical experience of confronting cyber threats.

Increasingly, Original Equipment Manufacturers (OEMs) understand this problem and are prioritizing cybersecurity, and trying to also embed cybersecurity within the component suppliers.

A lot of effort is now being focused on closing this gap within the automotive sector, and progress is being made. The desire to innovate and deploy new technologies must be tempered by an understanding of the cybersecurity vulnerabilities they may create, especially in traditional automotive businesses now re-engineering their design processes for a new generation of smart vehicles. This requires greater levels of co-operation and collaboration between the innovators and cybersecurity experts, incorporating concepts such as privacy-by-design and security-by-design from the very start.

Section

4



Emergency service: responding to an attack

Organizations are wise to operate on the basis that it will only be a matter of time before they suffer an attack that successfully breaches their defenses. Having a cyber breach response plan (CBRP) that will automatically kick in when the breach is identified represents an organization's best chance of minimizing the impact. But a CBRP must span the entire organization and it must be led by someone with the experience and knowledge to manage the organization's operational and strategic response. The CBRP framework will span:



Cybersecurity

How will the organization ensure it withstands the attack, isolates and assesses the damage done, and shores up defenses to prevent similar breaches in the future?



Business continuity planning

How will the organization continue to operate as normal while remedying the attack?



Compliance

What are the organization's duties for reporting the breach to the appropriate authorities, including law enforcement agencies if necessary, and how will these be discharged?



Insurance

Does the organization have cyber insurance and is this incident covered? In which case, what can be claimed?



Public relations and communications

How will the organization communicate clearly and effectively with all potential stakeholders, including employees, customers, suppliers and investors, both directly and via the media where there is public interest in the breach?



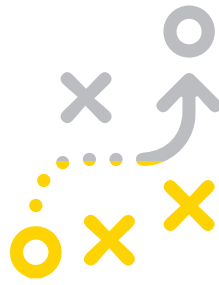
Litigation

How will the organization assess what potential litigation the attack leaves it vulnerable to, or even whether it has any recourse to legal action itself? How will it forensically record and maintain evidence for use by law enforcement agencies?

In practice, the CBRP is effectively a crisis management plan. It is required to provide guidance to every function of the organization involved in the response, set a level of understanding about what information is critical for senior leaders to know – as well as when and how to express it – and underpin the precision and the speed of the organization's continuous reaction as the breach continues to unfold – possibly over days, weeks or even months.

This survey suggests different levels of readiness among organizations. Many organizations may also be confused about their legal responsibilities – 17% of respondents say they would not notify all customers, even if a breach affected customer information; 10% would not even notify customers impacted. As the European Union's General Data Protection Regulation looms large, such positions will not be justifiable.

Overall, while 69% of respondents have some form of formal incident response capability; only 8% say describe their plan as robust and spanning third parties and law enforcement.



43%

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



56%

say they would make a public statement to the media within a month of a breach compromising data.



Coping with cloud and convergence

Traditional thinking about IT structures looks increasingly outdated: large numbers of organizations now depend on IT infrastructure, both software and hardware, that is hosted remotely in the cloud rather than on-premises; and the distinction between IT and operational technology (OT) is rapidly melting, as organizations link the two. Convergence and connectivity have become the norms.

There are good reasons for this. In the virtual environment of the cloud, there are no constraints on users from physical limits and infrastructure is easily adapted and scaled. Connecting IT to OT can drive end-to-end processes that transform productivity in every area of the organization.

Equally, however, these themes pose major cybersecurity headaches. With organizations maintaining virtual structures composed of multiple entities, no configuration can be more secure than its weakest link – and there are ever more links to protect. An attack on one link, moreover, rapidly becomes an attack on the entire organization.

Organizations must now understand this reality and take steps to mitigate the risks posed. In particular, the concept of zoning is crucial here: inevitably, in a large network of connected systems, some areas will be more vulnerable than others, and some will contain more valuable assets and systems; identifying and then protecting these zones with enhanced security must then be a priority.

The aim is to build firebreaks between different areas of the network – to ensure that convergence within the organization does not provide convenience for cyber attackers. The fact that an attacker is able to penetrate one zone should not mean that access to all other zones becomes straightforward – and particularly that there is no additional risk of compromise for high-value areas.



Section

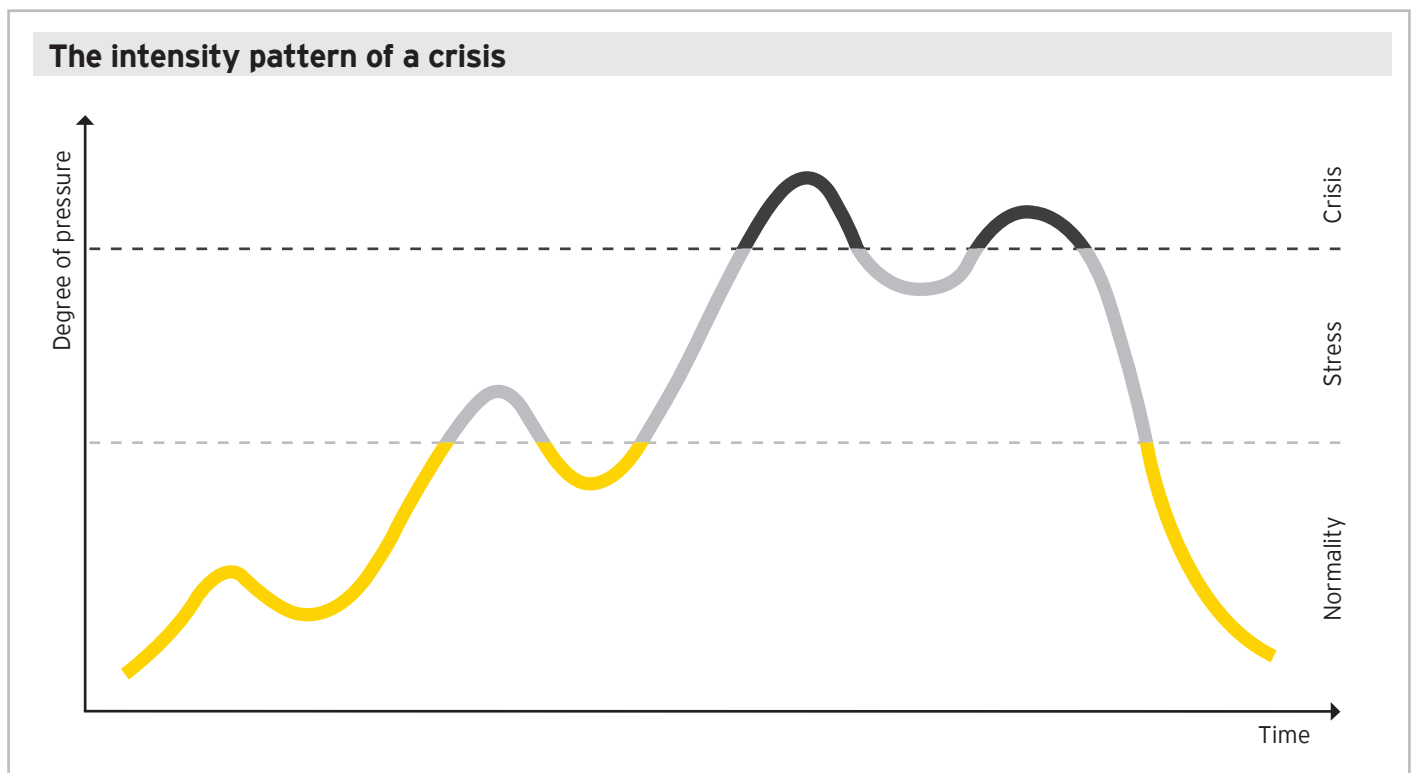
5



Conclusion

In previous editions of this survey, the need to structure cybersecurity resilience around the principles of detect, protect and react has been highlighted. These imperatives are more important than ever: organizations that understand the threat landscape and have strong defenses in place will stand a greater chance of repelling attacks and identifying those attackers that do get through; those with the ability to fight back will limit the damage attackers can do by acting quickly.

It may be helpful to think about cybersecurity in the context of crisis management. As the chart demonstrates, organizations confronted by major events or incidents must manage peaks of pressure as the problems ramp up stress levels and trigger a full-blown crisis.¹¹



¹¹ "Report on Cyber Crisis Cooperation and Management", European Union Agency for Network and Information Security, November 2014.

Actions all organizations should consider

Threat type	Strategy	Example activities
<p>Common attacks</p>	<p>Organizations need to be able to prevent these types of attacks through good basic cybersecurity.</p>	<ul style="list-style-type: none"> ▶ Establish governance and organization – understand key business drivers and obtain senior management support for a robust cybersecurity program; establish roles and responsibilities; agree strategy, develop policies and standards; enable reporting. ▶ Identify what matters most – map business objectives/products/services to supporting people, processes, technology and data infrastructure, and rank by criticality to your business. This includes the ecosystem/supply chain in which you operate: both third parties who supply you and those that you supply. ▶ Understand the threats – understand who might want to attack you, why, and how they might carry out an attack; focus your efforts on how to respond to the most likely threats. ▶ Define your risk appetite – understand what the most likely cyber attacks could cost your business through simplified cyber risk quantification coupled with a cyber risk management framework, which forms part of your overall operational risk management processes; set your risk appetite and reporting mechanisms to ensure you operate within it. ▶ Focus on education and awareness – establish an education and awareness program, ensuring all employees, contractors and third parties can identify a cyber attack and are aware of the role they play in defending your business. ▶ Implement basic protections – secure your business at the technology level by deploying basic protections including secure configuration, patch management, firewalls, anti-malware, removable media controls, remote access controls, and encryption; establish a Vulnerability Management (VM) program which manages vulnerabilities from identification through to remediation; establish an effective Identity and Access Management (IAM) program to control access to your information; focus on data protection and privacy (technical and compliance) as well as managing third parties who have access to/control of your data.

Actions all organizations should consider

Threat type	Strategy	Example activities
Advanced attacks	Organizations need to prevent some of these attacks, but focus on their ability to detect and respond to the more sophisticated and dangerous attacks.	<ul style="list-style-type: none"> ▶ Be able to detect an attack – establish a security monitoring capability that can detect an attack through monitoring activity at various levels within your business; this could be a basic system whereby an alert is generated and emailed when suspicious activity is detected on a firewall, through to a 24x7x365 Security Operations Center (SOC) monitoring networks, operating systems, applications and end users. ▶ Be prepared to react – establish a formal cyber incident management team who have been trained in and are following a documented plan, which is tested at least annually. ▶ Adopt a risk-based approach to resilience – establish recovery plans (including comprehensive backups) for all processes and supporting technologies in line with their criticality to the survival of the business. ▶ Implement additional automated protections – mature existing capabilities (for example, automate VM and IAM processes using specific technology), in addition to implementing complimentary capabilities/technologies such as Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Web Application Firewalls (WAF) and Data Loss Prevention (DLP) systems. ▶ Challenge and test regularly – carry out a cyber incident simulation exercise to test your executive management’s ability to manage the response to a significant cyberattack; carry out an initial red team exercise (a planned attack, carried out by professional ethical hackers) to test your technical ability to detect and respond to sophisticated attacks. ▶ Create a cyber risk management life cycle – reflect on all areas of your cyber risk management program and identify areas for ongoing improvement; repeat risk assessments on a regular basis; consider compliance with relevant regulations.
Emerging attacks	Organizations need to understand the emerging threats and how they should impact strategic decision-making, while making focused investment in cybersecurity controls.	<ul style="list-style-type: none"> ▶ Build security into the development life cycle – ensure cyber risk is considered in all new products, services, business ventures, etc., completing risk assessments as required and managing within agreed risk appetite. ▶ Enhance threat monitoring – use forward-looking threat intelligence to identify and track emerging threats.

Understanding the threat landscape – detecting the potential risks on the horizon – is the groundwork of good cybersecurity. It enables organizations to limit the time they spend outside normality, to understand when and why they have moved into stress, and therefore to pre-empt the development of a full-on crisis.

Fighting back – protecting the organization from cyber risk – builds on this groundwork. It gives the organization the skills and confidence to deal with stress and crisis more effectively, with tools and processes that provide a framework for responding to attackers.

The ability to respond to an attack – to react quickly and effectively when a breach does occur – is the final piece in

the puzzle. Such a breach, whether a compromise of data or an attack on an organization’s controls systems, will almost certainly represent a full-blown crisis. But organizations able to act calmly, employing a well-thought-out and tested cyber threat breach response plan in which everyone understands their responsibilities, will be able to de-escalate the crisis much more quickly.

By pulling these strands of cybersecurity together, organizations will move toward greater resilience, even in the face of the significant and increasing risk posed by diverse and often sophisticated cyber attackers. The tools and technologies required to meet the threat are already available and many organizations have developed innovative policies and processes to make best use of them. Now this best practice must become standard for all organizations.

Section

6



Survey methodology


















EY's 20th Global Information Security Survey captures the responses of nearly 1,200 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 June-September 2017.

Respondents by area















■ EMEIA	41%
■ Japan	7%
■ Americas	37%
■ Asia-Pacific	17%





















Respondents by number of employees

Less than 500		30%
501-1,000		11%
1,001-2,000		12%
2,001-3,000		6%
3,001-4,000		5%
4,001-5,000		5%
5,001-8,000		7%
8,001-10,000		4%
10,001-15,000		5%
15,001-20,000		2%
20,001-30,000		4%
30,001-40,000		2%
40,001-50,000		1%
50,001-75,000		2%
75,001-100,000		1%
100,001-150,000		1%
More than 150,00		1%

Respondents by total annual revenue (in USD)

Less than 1 Million		4%
1 Million-5 Million		5%
5 Million-10 Million		3%
10 million-50 million		7%
50 million-100 million		6%
100 million-500 million		18%
500 million-1 billion		12%
1 billion-1.5 billion		4%
1.5 billion-2 billion		5%
2 billion-5 billion		14%
5 billion-10 billion		8%
More than 10 billion		14%

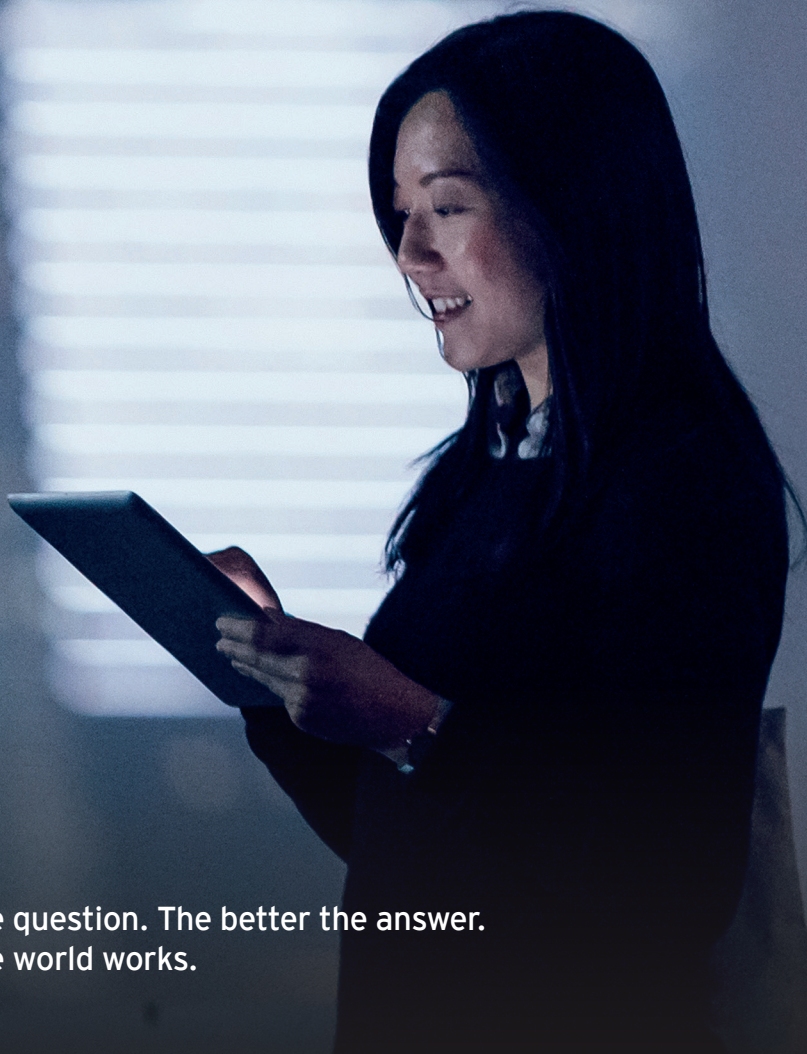
Respondents by industry sector

Aerospace & Defense		1%
Automotive & Transportation		6%
Banking & Capital Markets		14%
Chemicals		1%
Consumer Products & Retail		12%
Diversified Industrial Products		6%
Government & Public Sector		7%
Health		3%
Insurance		7%
Life Sciences		2%
Media & Entertainment		3%
Mining & Metals		3%
Oil & Gas		4%
Power & Utilities		5%
Professional Firms & Services		3%
Real Estate		3%
Technology		6%
Telecommunications		4%
Wealth & Asset Management		3%
Other		8%

Is your business fit for a digital world?

Digital creates opportunities
and risks across the value chain.
Discover how looking at digital
from every angle can help grow
and protect your business.

ey.com/digital #BetterQuestions



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



Building a better
working world

Contacts

For questions about EY 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 1592 bob.sydow@ey.com

Brian Loughman +1 212 773 5343 brian.loughman@ey.com

EMEA

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

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

Asia-Pacific

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

Chris Fordham +852 2846 9008 chris.fordham@hk.ey.com

Japan

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

Ken Arahari +81 3 3503 1100 ken.arahari@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.

© 2017 EYGM Limited.

All Rights Reserved.

EYG no. 06574-173Gbl

BMC Agency
GA 1006314

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