Insights on governance, risk and compliance

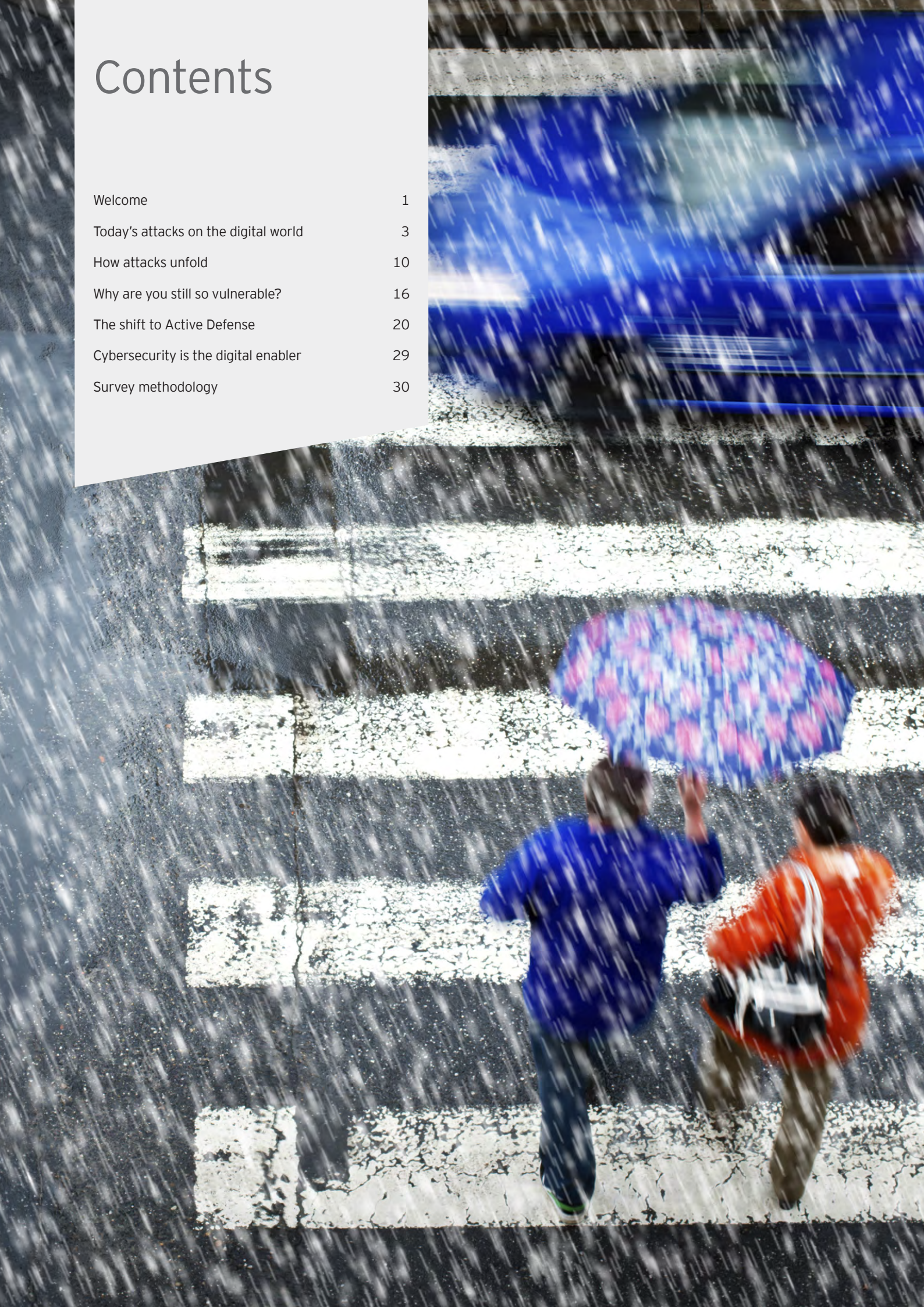
Creating trust in the digital world

EY's Global Information Security Survey 2015

EY

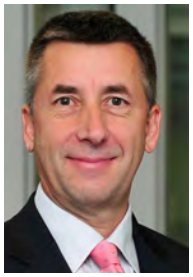
Building a better working world

Contents



Welcome

Paul van Kessel
EY Global Advisory Risk Leader



Ken Allan
EY Global Advisory Cybersecurity Leader

Welcome to *Creating trust in the digital world*, EY's Global Information Security Survey (GISS) 2015, our 18th annual survey, which investigates the most important cybersecurity issues facing businesses today.

This year, we were pleased to have 1,755 organizations participate in the survey, and this report is based on insights extracted from the results and from our extensive global experience of working with clients on improving their cybersecurity solutions.

Last year, we identified the ways organizations could get ahead of cybercrime by following a three-stage journey — Activate, Adapt and Anticipate. This concept still applies, but as cyber attackers are continuously changing tactics, increasing their persistence and expanding their capabilities, the nature of the cyber threats has evolved. Cyber attackers are today finding new and better ways to take advantage of the rapid expansion of digitization and the increasing connectivity of businesses, and the ways in which our personal lives are more and more interwoven with mobile technologies and the internet.

If you are struggling to understand how you can manage this situation, you are not alone — more than one-third of participants in our survey still think it unlikely they would be able to identify a sophisticated cyber attack — and, from our experience, we know that only the most vigilant of organizations would be able to spot the small anomalies that are indicative of a long-term breach.

Cybersecurity is more than a technology issue, and it cannot remain in the IT domain. It also cannot be the responsibility of any one member of the board — it affects every level of a business and every part of the C-suite in different, often subtle and not easily recognized, ways. This report looks at how various parts of an organization need to come together and share experiences in order to accumulate evidence to identify where attackers have already gained access and are even now gathering information that could strike at the core value of your organization.

Your aim should continue to be getting one step ahead of the cyber attackers, which today means learning how to be in a constant state of "Active Defense". In this report we explore what that means, and how EY can help you do that.

We would like to personally thank our clients for devoting their time to completing the survey, and we hope you enjoy reading this report.

Paul van Kessel
EY Global Advisory Risk Leader
paul.van.kessel@nl.ey.com

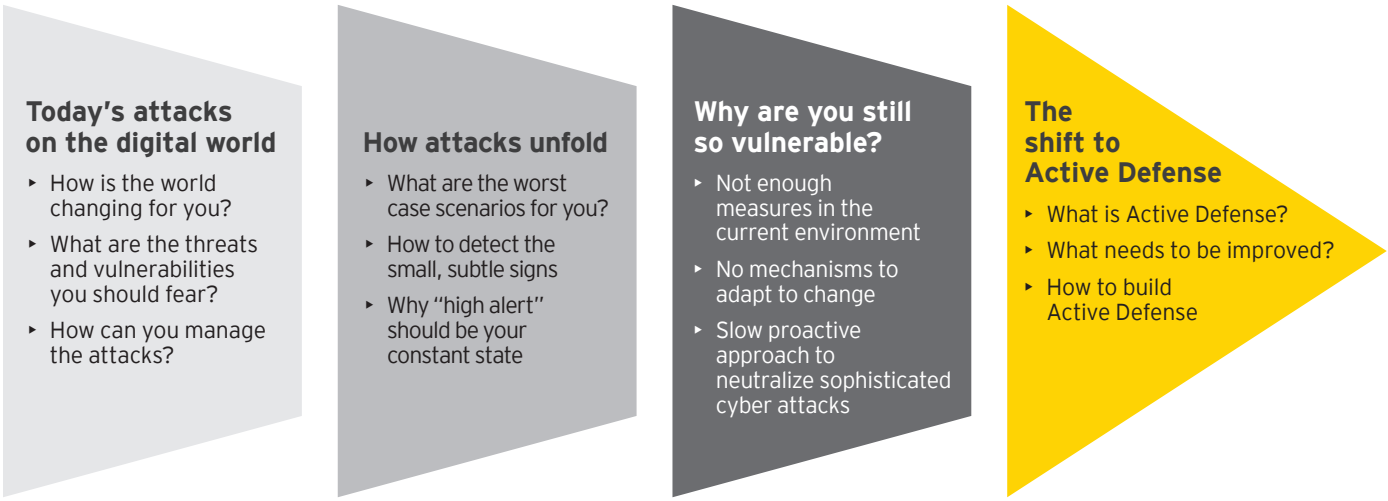
Ken Allan
EY Global Advisory Cybersecurity Leader
kallan@uk.ey.com

Understanding the challenges for cybersecurity

The digital world abounds with rapidly expanding opportunities for innovation, and businesses, governments and individuals have turned their attention to the significant benefits. By creating new markets and new products, a better understanding of consumers and citizens and finding different ways of connecting with them, the digital world offers enormous potential.

Unfortunately, in the rush, many precautions have been overlooked and risks underestimated. The realization that there is a flip side, and that the digital world also offers great potential for exploitation by criminals and others wanting to cause trouble, has come too late. In addition, complex, unintended consequences from the interconnectivity between people, organizations and "things", are starting to emerge.

For organizations to recognize the current challenges and to understand what they need to do to, they need to think fully about each of the following four areas:



Today's attacks on the digital world

88%

of respondents do not believe their information security fully meets the organization's needs

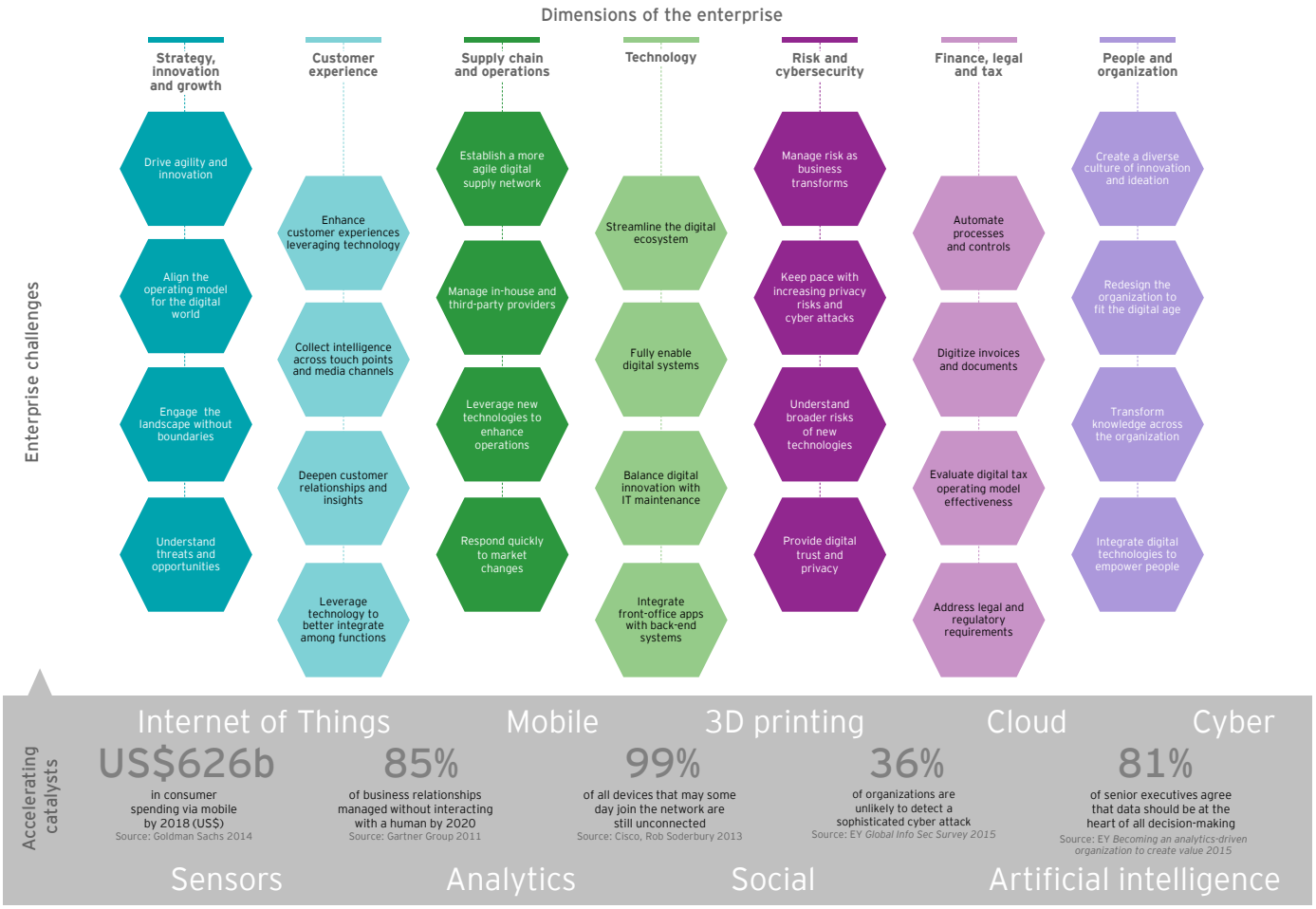
How is the world changing for you?

Organizations have no choice but to operate in this evolving environment so, inevitably there is a growing focus within governments and the media on what is going wrong where cyberspace meets the physical world. Customers having their personal details stolen and used is unacceptable, and the theft of intellectual property is understood to be detrimental to prosperity, as is the burden of the losses and the subsequent costs of remediation. The hacking and manipulation of media, communications, government administration and defense systems is seen as a significant threat to national security.

So how well do you understand what surviving in the digital world means for you and your organization?

Your whole organization needs to be viewed in the "cyber" dimension, and all these areas need to be considered:

Harnessing cybersecurity for digital opportunity and sustainability



Operating in a digital world — what is new?

- "Smart" devices and services resulting in unintended consequences and a mass of data, increasing vulnerabilities for exploitation; humans often removed from decision making processes
- Social media and BYOD, with employees, customers, citizens "always on" and sharing information — not fully appreciating the implications for privacy and confidentiality
- Organizations putting more data in the cloud and with third parties; attractive, but dangerous, with the loss of control, increased threats and unexpected connectivity — creates a complex ecosystem
- Human behaviors are changing, in both positive and negative ways
- Rafts of new legislation and regulations are forcing a change in processes. These, in turn, mean that other vulnerabilities are created, which further change the threat landscape (often widening, not reducing) and the attack surface of an organization

68%

of respondents do not consider monitoring their business ecosystem as an information security challenge in the Internet of Things

What are the threats and vulnerabilities you should fear?

For your organization to move to a safer and more sustainable place in the digital world, it is necessary to apply a cyber-risk lens to everything you do.

Too many organizations are taking an ad hoc approach to managing their risks and vulnerabilities, exposing us all to greater threats. This is not a responsibility that can be delegated to one or two individuals; rather, a wide range of individual responsibilities must be noted and detailed throughout the organization and your broader ecosystem, and brought together to form a single coherent and accessible view. This view will look different for the board and the C-suite than for employees, just as it will appear different again for partners, suppliers, vendors and other third parties.

The problem is managing how not to drown in all this data and create more work and risks than it is worth. Instead, you should prioritize, streamline and map out what a comprehensive and efficient cybersecurity approach means for your particular organization. The basic building blocks may be common (as outlined in our 3As approach — see www.ey.com/GISS2014), but you will only get true value by tailoring your cybersecurity approach to your business strategy, risks and priorities.

To then efficiently guide your organization through the layers of risks and threats, leaders must have the confidence to set the risk appetite and be prepared to swing into decisive action to handle any incidents. For example, one clear theme emerging from the last couple of years is that the impact of an incident is greatly reduced by the leadership ensuring there is intelligent and appropriate handling of cyber incidents and effective communication both internally and externally to manage the outcome.

67%

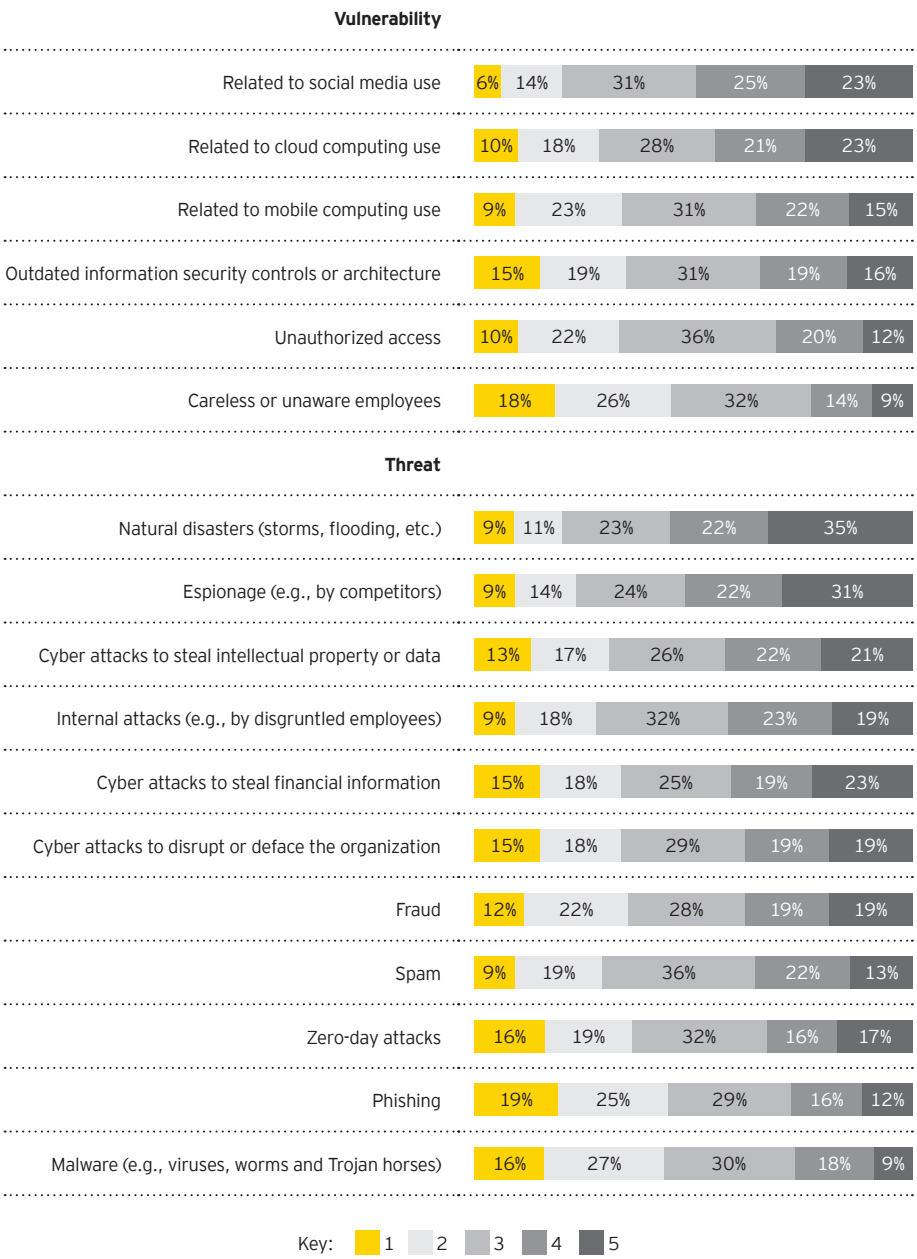
of respondents do not see managing the growth in access points to their organization as an information security challenge in the Internet of Things

Questions for your organization to consider:

- Do you really have confidence in your understanding of the threats/vulnerabilities in the digital world?
- Have you done the work and thinking required to determine how that threat landscape applies to your organization and strategy and prioritized cybersecurity measures around this?
- Do you know how to set your risk appetite to determine the acceptable and unacceptable loss and harm from potential incidents as part of developing your cyber breach response management program?

Only when the risk appetite is set at a level the board is comfortable with, and the organization can achieve, will your digital transformations be sustainable.

Which threats* and vulnerabilities have most increased your risk exposure over the last 12 months?** (Rate all of these items, with 1 as the highest priority, down to 5 as your lowest priority)



**Threat* is defined as the potential for a hostile action from actors in the external environment
***Vulnerability* is defined as exposure to the possibility of being attacked or harmed exists

How does 2015 compare with 2014?

If we look at the top two vulnerabilities:

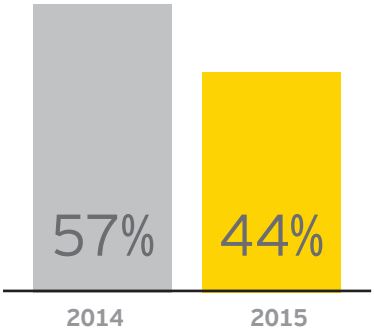
- Careless or unaware employees
- Outdated Information Security controls or architecture

In 2014 these same two vulnerabilities were perceived to be high and highest priorities, but the degree of vulnerability organizations feel has decreased in these areas. Today, only 44% feel vulnerable in relation to unaware employees, compared with 57% in 2014; only 34% feel vulnerable due to outdated systems, compared with 52% in 2014. This shows that organizations believe they are covering their vulnerabilities more effectively.

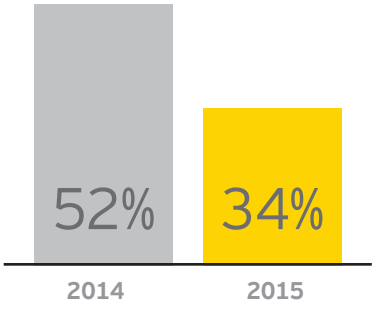
However, when we look at the top two threats today:

- Phishing
- Malware

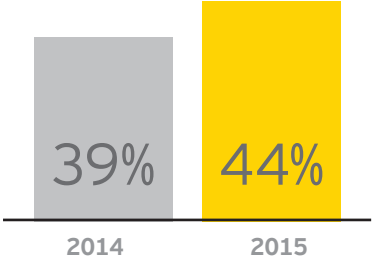
These threats ranked 5th and 7th in 2014, with the theft of financial information, IP, the threat of fraud, espionage and zero-day attacks all seen as higher. This much-heightened perception of phishing and malware as threats demonstrates a clear shift in perspective, but is it the correct shift or a swerve in the wrong direction?



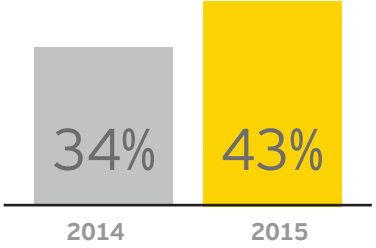
Today, only 44% feel vulnerable in relation to unaware employees, compared with 57% in 2014



Only 34% feel vulnerable due to outdated systems, compared with 52% in 2014



44% see phishing as the top threat today, compared with 39% in 2014



43% see malware as the top threat today, compared with 34% in 2014

42%

of respondents say that knowing all their assets is a key information security challenge

Can you stop the attacks?

Your organization will suffer cyber incidents. This is integral to the digital world.

The starting point for gaining confidence as an organization is situational awareness – an understanding of what you look like to a cyber attacker.

- How can you protect your organization against a cyber incident if you do not know what it is the attackers are targeting?
- How will they be able to gain access and how would this damage you and your critical assets?
- How can you have confidence if you do not fully understand your organization's ability to respond, contain and recover from an attack?

Organizations are often familiar with good risk management principles, and this is a useful starting point for thinking about cyber security:

Key risk management principles ...	... applied to cyber risk
1 **Focus on what matters most** Must align to your unique business and risk culture	**Know your critical information assets** Identify critical business assets most vulnerable to cyber attack
2 **Measure and report** Include qualitative statements and quantitative measures	**Make cyber risk more tangible** Clearly define cyber risk and underlying metrics
3 **Comprehensive in nature** Should cover all risk types, current and forward-looking	**Align with existing risk frameworks** Financial, operational, regulatory, customer, reputation, etc.
4 **Allocation of risk appetite** Allocation of appetite to business units and risk types	**Make cyber risk relevant to the business** Link organizational-level risks to individual BUs and their information assets
5 **Integrate with business planning** Regulators are increasingly looking for evidence	**Embed risk appetite in investment decisions** Prioritize investment where critical, empower businesses to make informed local decisions

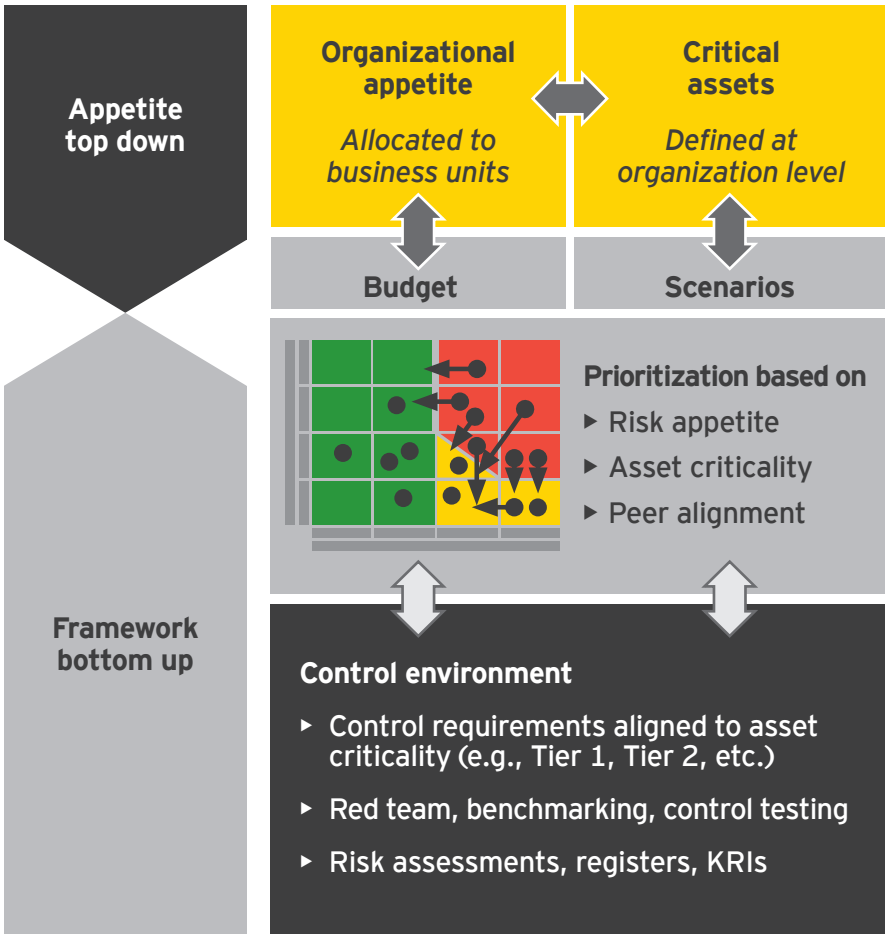
Cyber incidents are often announced as sensational and dramatic events – massive breaches, with systems and sites becoming inoperable, resulting in sudden consumer inconvenience or damage. The headlines focus on the large-scale events where millions of account details are stolen, reams of confidential information leaked on line, IP stolen and systems damaged.

However, the sudden nature of these headlines is misleading. Most of these attacks started weeks or months before, when the cyber criminals found their entry point and patiently started to explore, locate valuable assets and make their plans.

Furthermore, cyber incidents will not be a one-off, no matter how complex or simple, targeted or random they may be, or appear to be. The early subtle signs and the cumulative impact of repeated attacks must be understood and factored into your planning and risk appetite.

20%

of respondents cannot estimate the total financial damage related to cyber incidents in the last 12 months



Red teaming: *A red team is a group that actively challenges an organization to improve its security via specific exercises, such as penetration testing, social engineering, etc.*

Identify the real risks

- Top-down definition of risk appetite and critical information assets
- Map critical assets across systems and business (and third parties)

Prioritize what matters most

- Assume breaches will occur – improve controls and processes to identify, protect, detect, respond and recover from attacks
- Balance fundamentals with emerging threats and peer capabilities

Govern and monitor performance

- Regularly assess performance and residual risk position
- Measure leading indicators to catch problems while they are still small

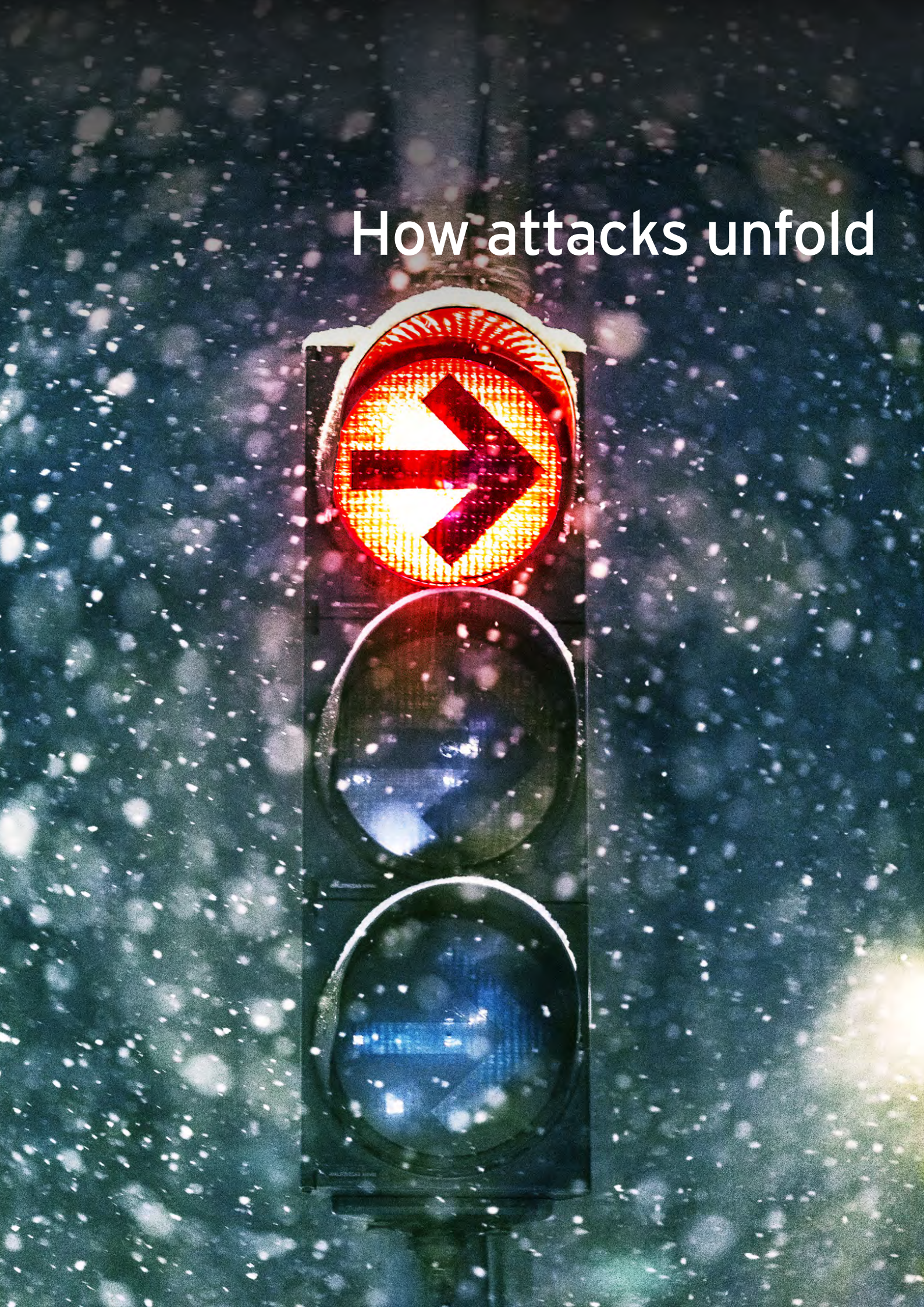
Optimize investments

- Accept manageable risks where budget is not available
- Ensure "on costs" and "Business as Usual" impact is considered for all investment

Enable business performance

- Make security everyone's responsibility
- Don't restrict newer technologies; use the forces of change to enable them

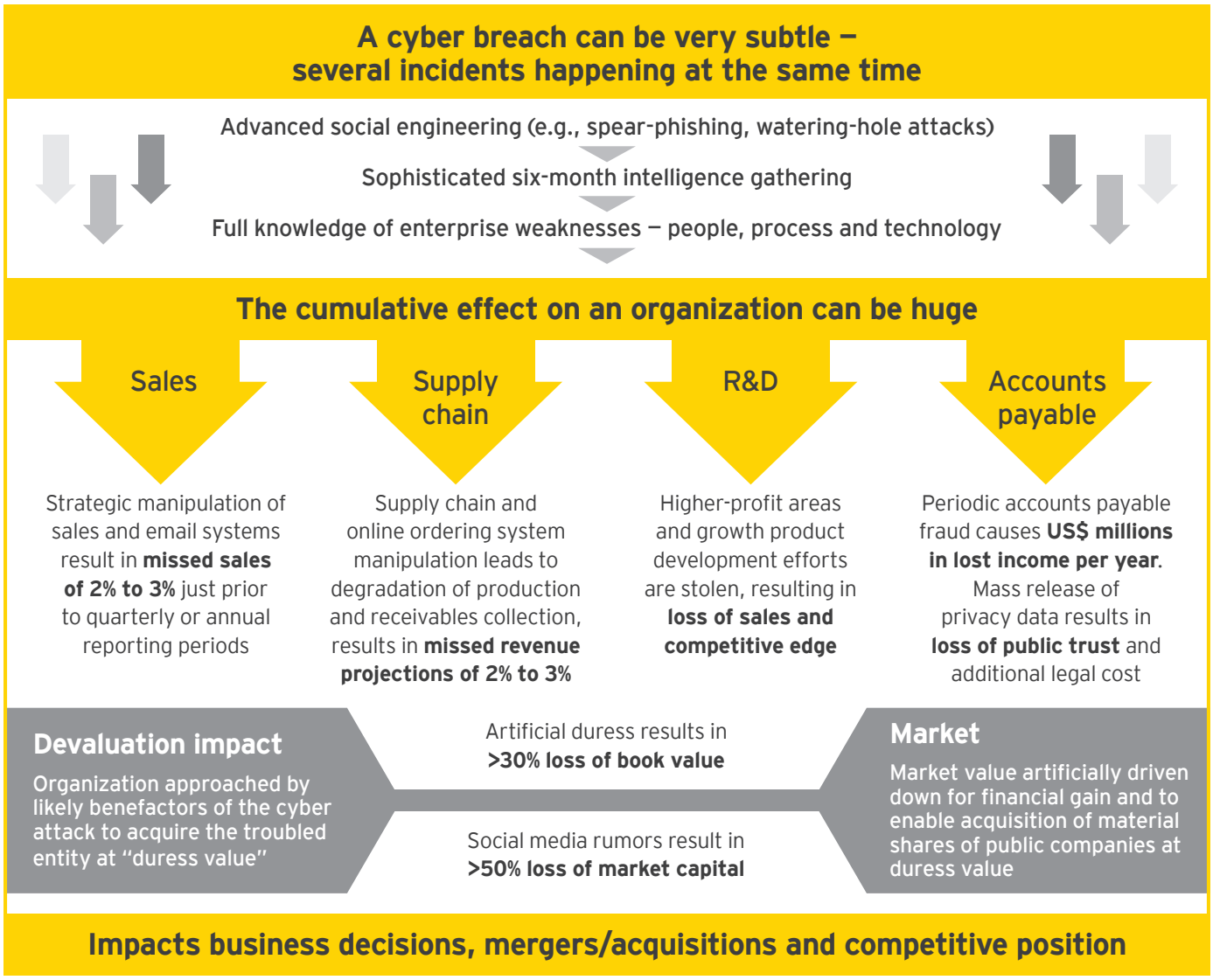
How attacks unfold



What are the worst case scenarios?

In order to identify that things are "not quite right," ... it is first necessary to know your environment inside and out – to identify what is critical to your organization's success, determine what some critical cyber business risk scenarios could be, and to build a picture of what would hurt the most if it were lost or compromised. Then you can prioritize your precautions and create counter-measures around those most critical areas and likely attack scenarios.

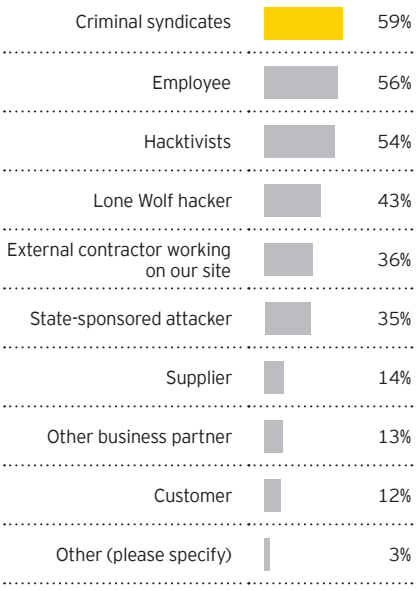
An example attack scenario:



With one or more top business and cyber-risk scenarios outlined, it is possible to identify which areas in the organization should be watched more carefully than others:

- Is it sales figures in a particular region where you suspect stolen IP is being used against you?
- Is it a fall in your market value over time as you are preparing for major M&A activity?
- Is it where you have a number of third-party organizations involved in a critical area of your business?

Who or what do you consider to be the most likely source of attack?



Are they in already?

Since cyber criminals can spend months inside your organization, finding information that they will store for a future attack or piecing information together that will get them to the prize they are after, they will also create measures to protect themselves from your detection. Sometimes they create diversionary tactics to draw your attention away from what they are doing and where they have succeeded. Often the criminals will keep the stolen information and not use it for a while – at other times, they will share it among the cybercriminal community (perhaps for a fee), spreading the direct threats to you even further.

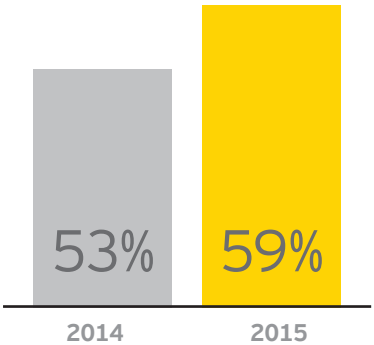
Occasionally, these criminal explorations will leave traces and tremors will be felt, but they are very easy to miss. The signs are so subtle that small disturbances in operations or apparently small glitches in systems don't get discussed or reported broadly, so no overall picture is collated. Even if cybersecurity is a standing item on the board of executives' agenda, it often won't become apparent that the small unexplained events each executive around the table is individually dealing with in his or her department may be part of a wider and sophisticated cyber breach that has the potential to do great damage.

How to detect the small, subtle signs

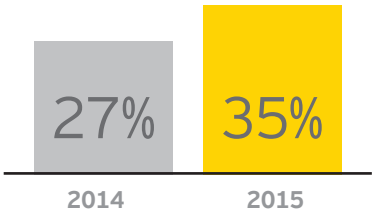
Placing the most attention, prevention and counter-measures around your areas of most value and highest risk is one key step in minimizing harm from cyber incidents. Being able to detect cyber incidents as early as possible is the next crucial step, which is only possible with a comprehensive radar that covers a variety of indicators and can raise alerts when a certain threshold is crossed. Determining the thresholds relates back to risk appetite and the sorts of incidents that will cause the most harm to your organization.

Some attacks will be sudden and obvious, in which case the whole focus switches to effective response. However, remember that these obvious attacks can also be a diversionary tactic, so organizations need the capability to analyze each incident in order to gain enough data to see patterns emerge over time.

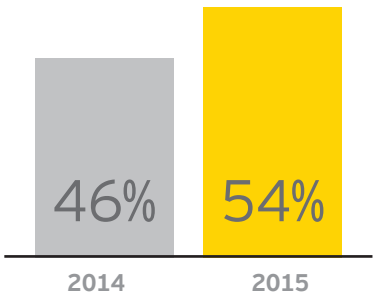
There are many ways into an organization, and cyber attackers will find the most vulnerable entry points. Some of these will be obvious and therefore easier to fortify, and they should be monitored, but from thinking creatively in a scenario about how the attackers could operate, additional barriers and monitors can be added in the not-so-obvious places (for example, public-facing websites, third-party systems that connect into yours, connecting industrial systems, the cloud, etc.).



59% see criminal syndicates as the most likely source of an attack today, compared with 53% in 2014



35% see state-sponsored attackers as the most likely source today, compared with 27% in 2014



54% see hacktivists as the most likely source today, compared with 46% in 2014

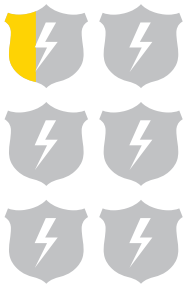
Once in, the attackers will make their way to the "value" points. This is where knowing your business priorities, what could hurt you (the most), and what has value to another party is essential — where they intersect is where more subtle indicators or signs may be detectable.

The Finance department, Marketing, Operations, R&D, HR — all of these key areas should be aware of the cyber business risks to the organization included in the range of individual responsibility areas. They all need to be alert for oddities in behavior and ready to raise these with the relevant cyber contact so they can add it to their other reports.

As with public counterterrorist campaigns, the message is that it will not hurt to report something that raises suspicions. The critical factor is that it is reported to the relevant parties who are able to piece together the jigsaw.

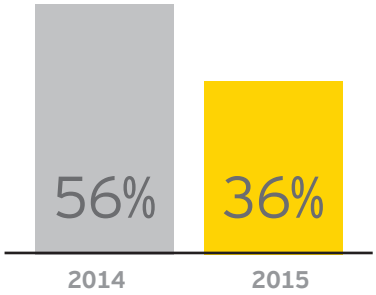
Examples of indicators that a radar should be tuned to detect are:

- Very visible attacks without an obvious purpose: e.g., DDoS; details stolen but with no obvious use to them
- Unexpected share price movements
- New products launched by competitors that are uncannily similar to your R&D and IP and reach the market just before yours — indicating IP theft and knowledge of your growth strategy and timings
- Mergers and acquisition (M&A) activities disrupted: rival bids that show similarities and may demonstrate awareness of confidential plans; M&A targets suffering cyber incidents (e.g., their IP stolen)
- Unusual customer or joint venture behavior: remember that these may not always be genuine customers or partners since cyber criminals can join organizations to to gain easier access to your systems and data
- Unusual employee behavior: managers of staff need to be more aware of changes in behavior, especially when those staff work in more sensitive areas
- Operational disruption but without a clear cause
- Oddities in the payment processing or ordering systems
- Customer or user databases showing inconsistent information



7%

of organizations claim to have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerability management function



36% say it is unlikely they would be able to detect a sophisticated attack. This is a significant improvement from the 2014 finding of 56%, but organizations need to remember that the level of sophistication is continually increasing

56%

of respondents defined data leakage/ data loss prevention as a high priority for their organization over the next 12 months

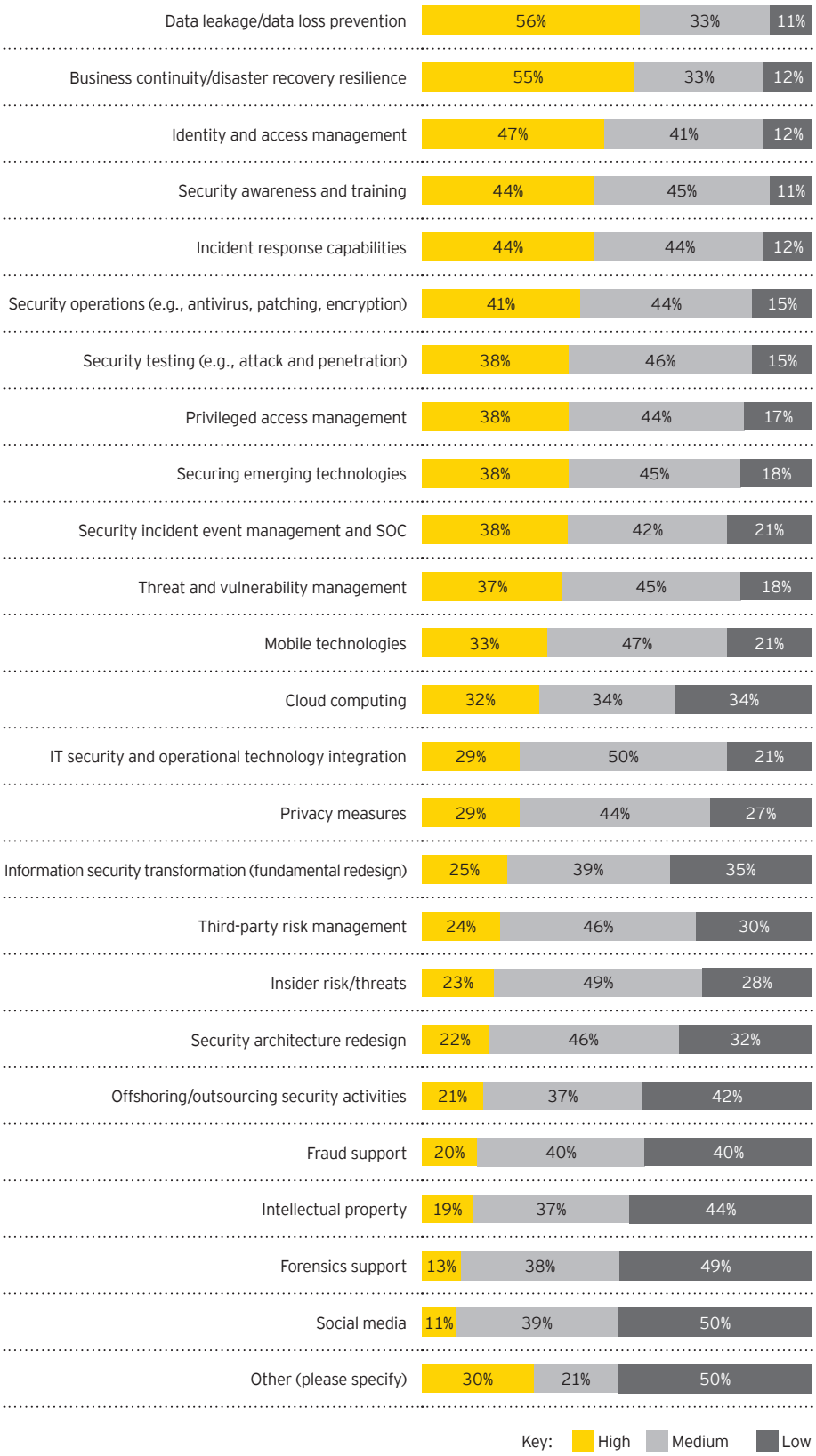
49%

49% of respondents defined Insider risks/threats as a medium priority, despite 56% saying employees are one of the most likely sources of an attack, and 36% naming onsite external contractors as a likely source

50%

of respondents defined social media as a low priority

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 topic)



Why "high alert" must be your constant state

The digital world does not allow any organization to feel comfortable in the area of cybersecurity threats and vulnerabilities. A constant guard that is on the alert, detecting and responsive to the changing environment, is essential. A non-stop, 365, 24/7 state of preparedness is essential.

But with this degree of vigilance, it is understandable that some organizations are feeling fatigue in this area, and many ask "when will it be enough?"

The constant bombardment of three to four years of numerous attacks and having to react to cyber events can easily provoke complacency. A strong record in repelling humdrum "typical attacks" (e.g., phishing) and plugging the obvious gaps (e.g., Identity and Access Management functioning effectively) can lead organizations to think they have "solved" the problem of cybersecurity, when in reality the situation is getting worse. This is especially true as it can be very difficult to demonstrate the value of the investment in real terms when budgets are tight.

In reality, most organizations have been putting the foundations for adequate cybersecurity in place, not realizing that this is just the start, and the digital world requires a steady and responsive approach to investment. An organization can only consider that it has "enough" cybersecurity when the organization is always able to keep within the bounds of the established risk appetite.

However, as the maturity of an organization's cybersecurity increases, it does become easier to demonstrate the value of these investments. Providing more accurate cost assessments for the harm that various cyber-attack scenarios will cause can help justify continued investment and vigilance. Each time your Security Operations Center (SOC) or internal threat intelligence analysts identify an attack in very early stages, it is possible to demonstrate the value of this to the business by extrapolating the damage that otherwise would have been caused had the scenario played out to its worst case.

Similarly, the better your situational awareness, the easier it is to streamline and prioritize your spending. A lot of money is wasted on unnecessary controls or equipment that do not necessarily enhance your cybersecurity maturity in the areas where it is most needed.

49%

say an increase in funding of up to 25% is needed to protect the organization in line with management's risk tolerance

84%

will spend the same or less on information security for IP over the coming year

70%

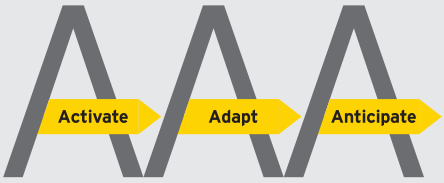
will spend the same or less on security operations (antivirus, patching, encryption, etc.)

62%

will spend the same or less on incident response capabilities over the coming year

Why are you still so vulnerable?

In our GISS 2014 report, we identified three stages of the journey to cybersecurity maturity – Activate, Adapt and Anticipate (the "three As") – that need to be executed in tight sequence with the aim of achieving ever more advanced and comprehensive cybersecurity measures at each stage.



The three As are still relevant, and our 2015 survey findings show that there is still progress to be made in all three stages. However, in the face of today's threats, many of the actions we identified as more advanced actions have now become more foundational.

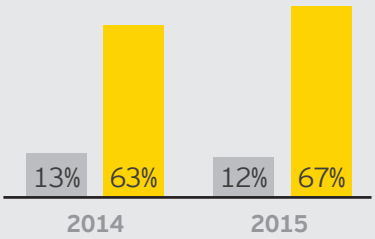
1. Activate

This is where an organization achieves a solid foundation of cybersecurity for the **current** environment, comprising a set of cybersecurity measures that help provide basic defense. It requires that the organization:

- Conduct a security assessment and create a road map
- Get board-level support for a security transformation
- Review and update security policies, procedures and supporting standards
- Establish a Security Operations Center
- Test business continuity plans and incident response procedures
- Design and implement cybersecurity controls

Today, with the cyber risks and threats having become more sophisticated, there are now two additional foundational tasks:

- Define the organization's ecosystem
- Introduce cybersecurity awareness training for employees

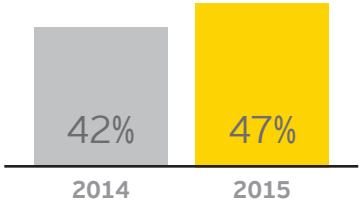


Percentage of respondents who believe their information security function fully meets the organization's needs; percentage of respondents who believe it partially meets the needs but are making improvements

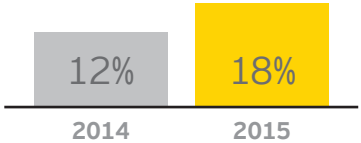
So where are businesses in 2015?

Not enough action in the current environment

- Only 12% currently believe that their Information security function fully meets the organizations' needs. 67% are still making improvements.
  - There has been a 1% drop in those who believe needs are being fully met, but the number making improvements has only risen by 4% since 2014.
- 69% say their information security budget needs to rise by up to 50% to protect the company in line with management's risk tolerance.
- 47% do not have an SOC, compared with 42% in 2014.
- 37% do not have a data protection program or only have ad hoc policies or processes in place, compared with 34% in 2014.
- 18% do not have an Identity and Access Management program while in 2014, this figure was 12% – this represents a serious drop.
- Only 40% hold an accurate inventory of their ecosystem (i.e., all third-party providers, network connections and data).
- 27% say that end-user phishing was the primary control or process failure leading to their most significant cyber breach in the last year.



Percentage of respondents who do not have a SOC



Percentage of respondents who do not have an IAM program

54%

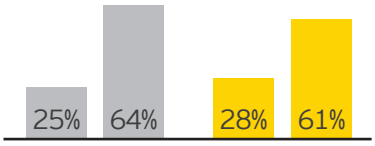
of organizations do not currently have a role or department in their information security function that is focusing on emerging technology and its impact

2. Adapt

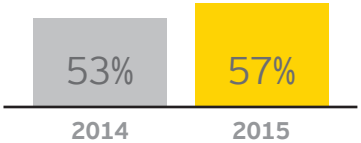
Accepting that foundational information security measures will become less effective over time, this stage focuses on the **changing** environment and highlights the actions necessary to ensure that organizations can continue to adapt to keep pace and match the changing business requirements and dynamics.

Today, the Adapt stage requires that they:

- Design and implement a transformation program to achieve a step improvement in cybersecurity maturity, using external help to accelerate or incorporate leading practice in designing the program and providing program management
- Decide what to keep in-house and what to outsource
- Define a RACI (Responsible Accountable Consulted Informed) matrix for cybersecurity



Percentage of respondents who intend to spend more on information security transformation or who intend to spend the same



Percentage who say that lack of skilled resources is challenging information security's contribution and value to the organization

So where are businesses in 2015?

Not enough adaptation to change

- 54% of organizations do not currently have a role or department in their information security function that is focusing on emerging technology and its impact – this includes 36% who have no plans to implement one.
- Only 34% would rate their security monitoring as mature or very mature, which is only a 4% increase on 2014.
- Only 53% would rate their network security as mature or very mature, which is only a 1% increase since 2014.
- 57% say that lack of skilled resources is challenging information security's contribution and value to the organization, while in 2014 this figure was 53%.
- When asked "compared to the previous year," 28% of responders said they planned to spend more on information security transformation (a fundamental redesign); this is only a 3% increase on responses to the same question in 2014.

3. Anticipate

At the Anticipate stage, an organization needs to proactively develop tactics to detect and neutralize potential cyberattacks. It must focus on the **future** environment and become more confident in its ability to handle more predictable threats, as well as unexpected attacks.

Few organizations are at this level of capability, and today it requires that they:

- Design and implement a Cyber Threat Intelligence strategy
- Define and encompass the organization's extended cybersecurity ecosystem
- Take a cyber-economic approach
- Use forensic data analytics and Cyber Threat Intelligence
- Ensure everyone understands what's happening
- Prepare for the worst by developing a comprehensive cyber breach response management strategy

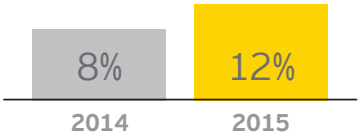
36%

of respondents do not have a threat intelligence program

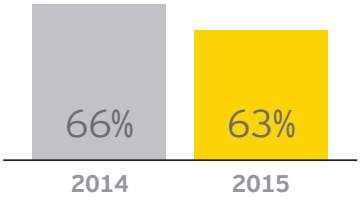
So where are businesses in 2015?

Slow proactive approach to neutralize sophisticated cyber attacks

- 36% do not have a threat intelligence program, with a further 30% only having an informal approach while 5% say that their organization has achieved an advanced threat intelligence function; compared with 2014, these figures have not changed, other than a drop of 2% in those who have the informal approach.
- 63% say threat and vulnerability management is a medium or low priority, which is only a marginal improvement on 2014.
- Only 12% look beyond their suppliers to their suppliers' suppliers (fourth parties), which is only a marginal improvement of 4% from 2014.
- Only 31% of all third parties are risk-rated and appropriate diligence applied, compared with 27% in 2014.
- 79% say that poor user awareness/behavior is the main risk associated with mobile devices.



Percentage of respondents who look beyond their suppliers to fourth parties



Percentage of respondents who say threat and vulnerability management is a medium or low priority

The shift to Active Defense

"Active Defense does not replace traditional security operations – it organizes and enhances them."

Ken Allan, EY Global Advisory Cybersecurity Leader

What is Active Defense?

Cybersecurity is an inherently defensive capability for organizations. Government defense departments (and the military) may be preparing offensive capabilities, developing cyber weapons and undertaking intrusive disruption activities, but for organizations outside of that narrow arena, offensive operations remain unnecessary and are often in a legal "gray zone."

However, that does not mean that organizations have to be passive and wait to become victims.

As described earlier in this report, understanding your critical cyber business risks and knowing what attackers may want from your organization enables you to establish "targeted defense" through prioritization (of assets, people, business areas) and hardening of vulnerabilities. And assessing the threat landscape particular to your organization (based on your operating environment, critical assets and business strategy) allows you to understand the most likely threat actors and methods they may use, which can be played out in scenarios to gauge readiness. This all informs your SOC and should be the basis on which it will support your organization.

Putting in place a more advanced SOC and using Cyber Threat Intelligence to effectively align operations helps enable you to conduct Active Defense by sending out intelligent feelers to look for potential attackers, analyze and assess the threat, and neutralize the threat before it can damage your organization's critical assets. Similarly, you can use an advanced SOC to operate in the same way and actively hunt down unwanted anomalies, "visitors" or confirmed attackers already in your systems.

24%

of respondents do not have a vulnerability identification program

34%

have an informal vulnerability identification program and perform automated testing on a regular basis

What needs to be improved?

Advanced Cyber Threat Intelligence: different levels of threat assessment and profiling can now be done, escalating from the more basic questions. More advanced Cyber Threat Intelligence enables you to proactively manage these threats and counter-measures.

Do you need to advance your Cyber Threat Intelligence?

Key questions to ask your information security function:

- What information about my organization/business is available to any attacker? How could they use it?
- What sort of attackers are my more likely adversaries (e.g., hacktivists, criminal networks looking for things to sell on, fraudsters, nation-state attackers)?
- What are their capabilities (e.g., likely resources, timeline, technical capabilities, ability to recruit insiders)?
- For each of the more likely adversaries, what are they likely to be interested in? (Match this to your list of what really matters to your organization/business – your "crown jewels.")
- How vulnerable are these desired targets/assets, and how could they be exploited?
- What specific paths might the adversaries take to their desired target (e.g., through an air-conditioning system, through a payment system, by recruiting an insider, by spear-phishing board members or targeted employees who have access)?
- What are the most effective counter-measures?
- What more can I learn from previous encounters with adversaries?

Armed with the answers to these questions, an organization would use the findings to inform strategic business decisions at executive and senior management level, re-focus operational activity in the SOC, and task the external threat intelligence feeds to the areas of most relevance for that point in time.

27%

say that data protection policies and procedures are informal or that ad hoc policies are in place

59%

of respondents say their SOC does not have a paid subscription to cyber threat intelligence feeds

How to build Active Defense

Active Defense extends traditional security operations capability in two key ways, but first it is guided by professionally analyzed Cyber Threat Intelligence. More than just receiving "feeds," actual analysis of threat intelligence allows Active Defense practitioners to identify likely attackers, infer their most likely targets within your business, and develop hypotheses about likely ways those attacks will unfold. This insight enables the implementation of tailored counter-measures.

The second key differentiator from the more standard cybersecurity approach is the Active Defense operational cycle. By iterating through a defined and disciplined process to analyze available information, draw relevant conclusions and take action, Active Defense practitioners can add a dynamic and proactive component to the organization's existing security operations.

Unlike other security service offerings, Active Defense isn't about improving a specific functional area or implementing new technologies. Instead, Active Defense integrates and enhances the enterprise's existing security capabilities to achieve greater effectiveness against persistent attackers. By implementing and executing an iterative cycle with built-in mechanisms for continuous learning and improvement, the organization can realize gains in efficiency, accountability and governance capabilities. These gains translate directly into an improved return on investment for security programs by increasing the effectiveness of security operations which, in turn, reduces the effectiveness of targeted attacks.

Active Defense should also include assessing the risk implications in the event of a major cyber breach and the development of a centralized response framework as part of the enterprise risk management strategy. The cyber breach response management framework, with a clearly defined governance model, should cover the process of incident investigation, evidence collection and analysis, impact assessment and litigation support.

Is Active Defense appropriate for your organization?

If the answer to any of these questions is "yes," you should consider an Active Defense approach:

- We have a SOC but are still not finding evidence of advanced attackers
- We have a SOC but still had a major breach
- We have an outsourced SOC, but our intellectual property and businesses systems are not truly secure

Your next steps toward building trust in a digital world

A simple answer to "what does my organization require?" is that it needs all of the following:

- Knowledge of what can hurt the organization and disrupt achieving your strategy
- Clear identification of your critical assets, or crown jewels
- Cyber business risk scenarios that paint an accurate picture of how an attack can progress
- A board and senior executives who can accurately determine the risk appetite for the organization
- An assessment of current cybersecurity maturity and a comparison with the maturity level that is actually required to meet the risk appetite
- An improvement road map
- Tailored threat profiling and advanced cyber threat intelligence
- A more advanced SOC: in-house, co-sourced or outsourced
- A proactive, multi-functional cyber breach response management strategy

To move forward on the cybersecurity road map and implementation plan could require a change in mindset in your organization and will require clarity around the board's role — a holistic solution and framework will be needed with complete alignment to your business performance. It is likely that external resources will be necessary to help your organization achieve this. Today, a board-level assessment of your current maturity spectrum could be an early and highly effective exercise to set the scene for the scale of change that might be required.

The following pages provide the complete spectrum of states of maturity — where are you today, and where do you think you need to be? The targeted defense approach does not suggest that the ideal state is essential in every aspect.

66%

percentage of respondents who had had a recent significant cybersecurity incident that was not discovered by their SOC say their SOC does not have a paid subscription to cyber threat intelligence feeds

The maturity spectrum — and where organizations currently rank

Maturity question	1 — Non-existent	2
What is the maturity of your threat intelligence program?	**36%** of respondents do not have a threat intelligence program	**30%** have an informal threat intelligence program that incorporates information from trusted third parties and email distribution lists
What is the maturity of your vulnerability identification capability?	**24%** of respondents do not have a vulnerability identification program	**34%** have an informal vulnerability identification program and perform automated testing on a regular basis
What is the maturity of your breach detection program?	**18%** of respondents do not have a detection program; a further **4%** do not have formal processes in place for response and escalation	**23%** have perimeter network security devices (i.e., IDS); a further **21%** utilize a security information and event management (SIEM) solution to actively monitor network, IDS/IPS and system logs
What is the maturity of your computer incident response capability?	**14%** do not have an incident response capability	**21%** have an incident response plan through which they can recover from malware and employee misbehavior; further investigations into root causes are not conducted
What is the maturity of your data protection program?	**10%** of respondents do not have a data protection program	**27%** say that data protection policies and procedures are informal or that ad hoc policies are in place
What is the maturity of your identity and access management?	**18%** of respondents do not have an identity and access management program	**25%** have a team with oversight of access management processes and central repository; conduct of reviews is not formally established

3	4	5 – Very mature
20% have a formal threat intelligence program that includes subscription threat feeds from external providers and internal sources, such as a security incident and event management tool	**10%** have a threat intelligence team that collects internal and external threat and vulnerability feeds to analyze for credibility and relevance in their environment	**5%** have an advanced threat intelligence function with internal and external feeds and dedicated intelligence analysts and external advisors that evaluate information for credibility, relevance and exposure to threat actors
20% use a variety of review approaches, including social engineering and manual testing	**18%** have a formal vulnerability intelligence function with a program of assessments based on business threats utilizing deep dive attack and penetration testing of suppliers, periodical testing of business processes and project testing (e.g., new systems)	**5%** have an advanced vulnerability intelligence function and conduct risk-based assessments with results and remediation agreed with the risk function throughout the year
6% have informal response and escalation processes in place; a further **5%** use ad hoc processes for threat collection, integration, response and escalation	**13%** have a formal detection program that leverages modern technologies (host-based and network-based malware detection, behavioral anomaly detection, etc.) to monitor both internal and external traffic	**11%** have a formal and advanced detection function that brings together each category of modern technology (host-based malware detection, antivirus, network-based malware detection, DLP, IDS, next-generation firewalls, log aggregation) and use sophisticated data analytics to identify anomalies, trends and correlations However, only **2%** have formal processes for threat collection, dissemination, integration, response, escalation and prediction of attacks
43% have a formal incident response program and conduct investigations following an incident	**16%** have a formal incident response program and established arrangements with external vendors for more complete identity response services and investigations	**7%** have a robust incident response program that includes third parties and law enforcement and is integrated with their broader threat and vulnerability management function; they also build playbooks for potential incidents and test them via tabletop exercises regularly
19% say that data protection policies and procedures are defined at the business unit level	**26%** say that data protection policies and procedures are defined at the group level	**17%** say that data protection policies and procedures are defined at the group level, reflecting corporate oversight and communicated through the business; specific business unit exceptions are documented, tracked and annually reviewed
34% have a formal team to provide oversight on defined access management processes although this is largely manual; a central directory is in place, yet it interacts with a limited number of applications and is not regularly reviewed		**23%** have a formal team that interacts with business units in gaining IAM oversight; they have well-defined processes, limited automated workflows, single source sign-on for most applications and undertake regular reviews

32%

of respondents stated that benchmarking information about the maturity of peer organizations was the most useful and their highest priority

Put your organization on the road to improvement

Few organizations today have the appropriate skills and resources in-house to effectively secure their information assets and at the same time optimize business performance. Organizations in all sectors can benefit from an objective assessment of their information security programs and structures.

An effective assessment should seek to assist your organization with:

- Understanding your organization's risk exposure
- Assessing the maturity of your current cybersecurity program and identifying areas for improvement
- Building a prioritized roadmap for project investments and organizational change initiatives
- Collecting information to create benchmarks against other organizations
- Validating that your security investments have improved your security posture

This assessment needs to be broad and high level, as well as totally immersive in specific areas and components, and this is where EY can help. Dashboard metrics help enable an organization to see what is needed to support the ongoing assessment, transformation and sustainability of the information security strategy.

Opposite is an example of maturity ratings that can help to position the organization along the relevant spectrum for its current, competitive and future states.

The effectiveness of information security

What are the main obstacles or reasons that challenge your information security operation's contribution and value to the organization? (Tick all that apply)

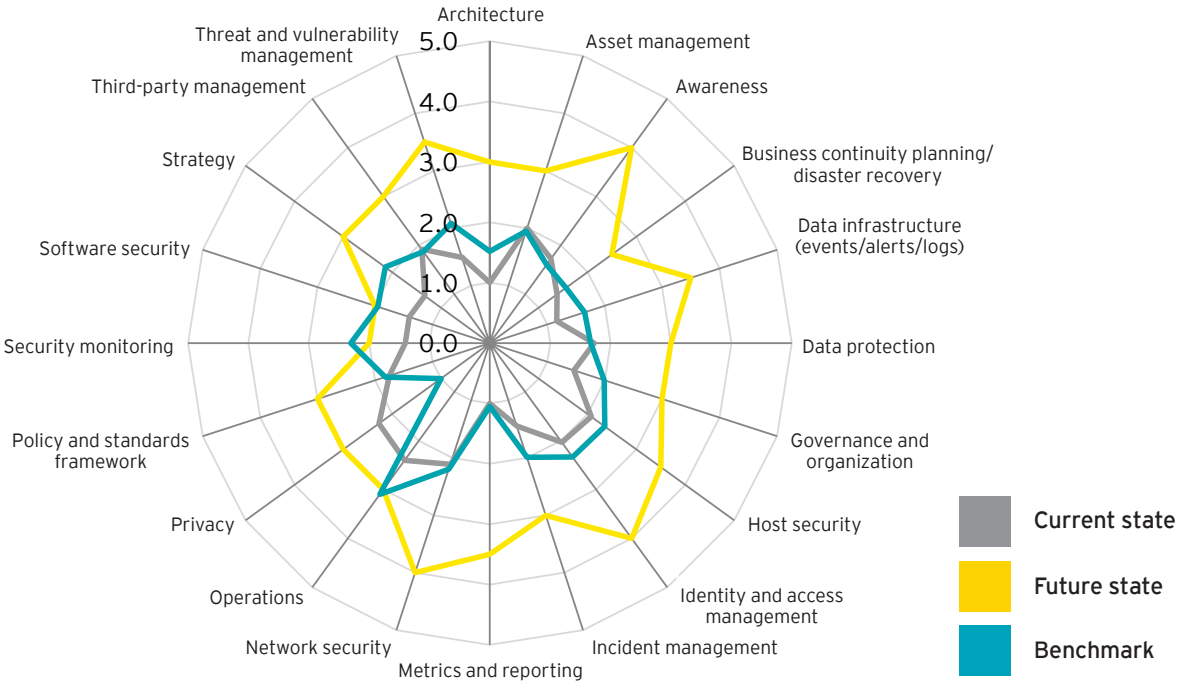
Do you have a RACI matrix?

With the board setting the tone and level of expectation, enterprise-wide collaboration is essential, as well as vigilance related to "how cyber risks and cyber attacks affect your role." Effective security management affects every role and every part of the organization; a RACI matrix, good governance and supportive employees are all essential – in our 3 As approach, it is a key element of the Adapt level of cybersecurity. Consider what a RACI matrix should look like for your organization, and be clear in the understanding that all cybersecurity is no longer only an IT issue.

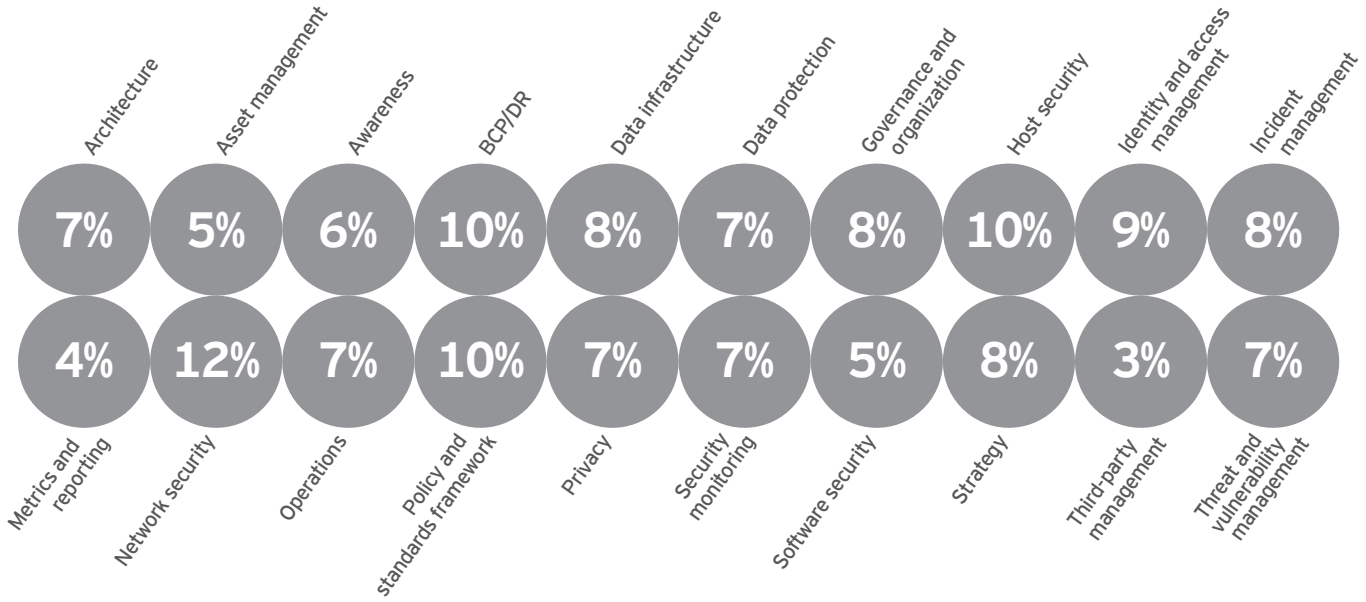
Current state cybersecurity maturity comparison between Organization X and its peers

X's current state maturity is approximately on the same level as in comparable peers. Defined future state increases the maturity level considerably.

Organization X versus peers



Percentage of respondents to our survey who indicated their level of maturity was "very mature"



Cybersecurity is the digital enabler

Cybersecurity is not an inhibitor in the digital world; rather it helps make the digital world fully operational and sustainable.

Cybersecurity is key to unlocking innovation and expansion, and by adopting a tailored organization and risk-centric approach to cybersecurity, organizations can refocus on opportunities and exploration. Building trust in a business that operates successfully within the Internet of Things (IoT), and that fully supports and protects individuals and their personal mobile devices (from a simple phone to a health care device, from smart appliances to smart cars), is a key to competitive differentiator and must be a priority.

By acting now, it is possible to adjust the balance of the digital world back toward sustainability and safety, to help better protect your organization and create trust in your brand.

Survey methodology

EY's *Global Information Security Survey* was conducted between June 2015 and September 2015. Participants included 1,755 respondents from 67 countries and across all major industries.

For our survey, we invited CIOs, CISOs, CFOs, CEOs and other information security executives to take part. We distributed a questionnaire to designated EY professionals in each country practice, along with instructions for consistent administration of the survey process.

The majority of the survey responses were collected during face-to-face interviews. When this was not possible, the questionnaire was completed online.

If you wish to participate in future EY Global Information Security Surveys, please contact your EY representative or local office, or visit www.ey.com/giss and complete a simple request form.

Profile of participants

1,755
respondents

67
countries worldwide

25
industry sectors

Respondents by area (1,755 respondents)

Key:

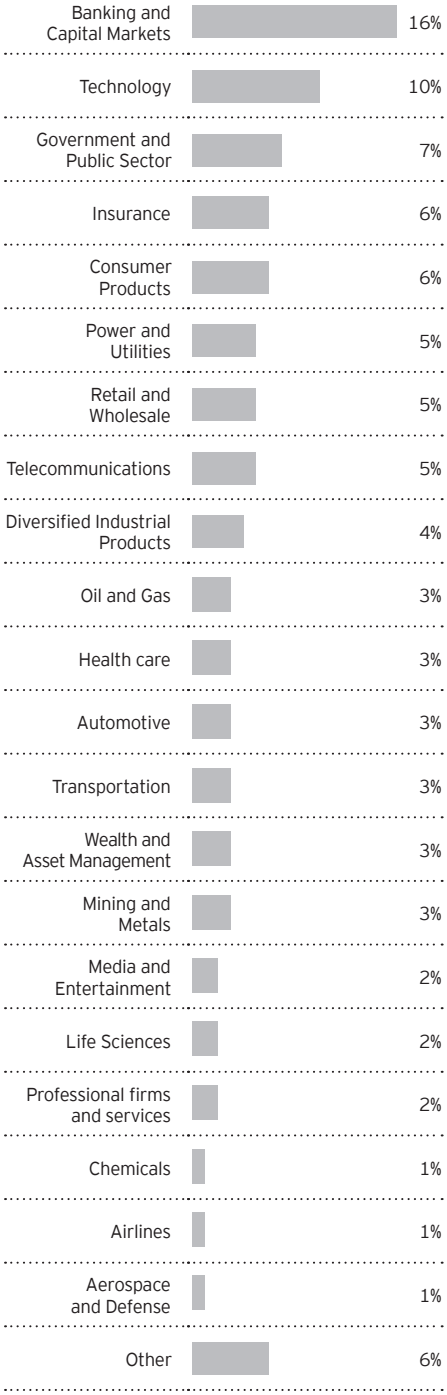
EMEIA	51%
Americas	29%
Asia-Pacific	15%
Japan	5%

Respondents by total annual company revenue

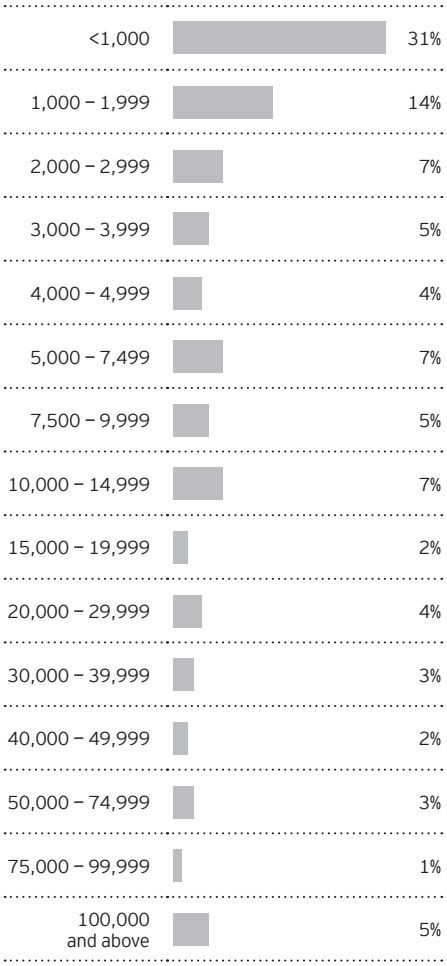
All amounts are in US dollars

Less than $10 million	5%
$10 million to <$25 million	5%
$25 million to <$50 million	4%
$50 million to <$100 million	6%
$100 million to <$250 million	9%
$250 million to <$500 million	9%
$500 million to <$1 billion	11%
$1 billion to <$2 billion	10%
$2 billion to <$3 billion	7%
$3 billion to <$4 billion	4%
$4 billion to <$5 billion	3%
$5 billion to <$7.5 billion	4%
$7.5 billion to <$10 billion	3%
$10 billion to <$15 billion	3%
$15 billion to <$20 billion	2%
$20 billion to <$50 billion	4%
$50 billion or more	3%
Government, nonprofit	6%
Not applicable	4%

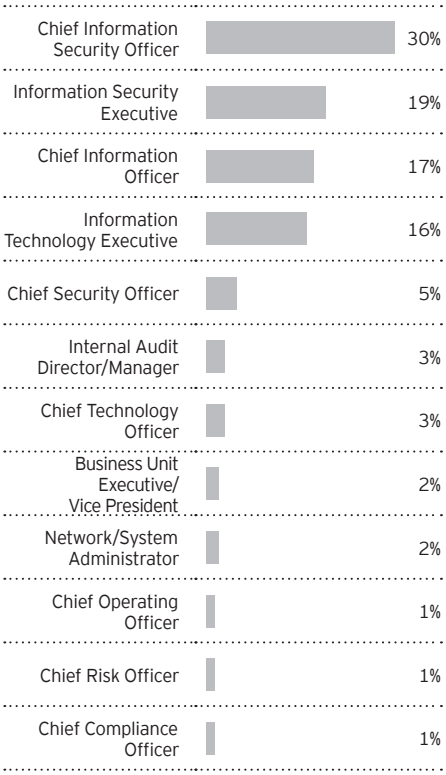
Respondents by industry sector



Respondents by number of employees



Respondents by position



Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective. Please visit our *Insights on governance, risk and compliance* series at www.ey.com/GRCinsights.

Cyber Threat Intelligence – how to get ahead of cybercrime

www.ey.com/CTI

Managed SOC – EY's Advanced Security Center: world-class cybersecurity working for you

http://www.ey.com/managedSOC

Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Get ahead of cybercrime: EY's Global Infomation Security Survey 2014

www.ey.com/GISS2014

Cybersecurity and the Internet of Things

www.ey.com/IoT

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

www.ey.com/3SOC

Cyber Program Management: identifying ways to get ahead of cybercrime

www.ey.com/CPM

Cyber breach response management – Breaches do happen. Are you ready?

www.ey.com/cyberBRM

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 deliver outcomes that grow, optimize and protect our clients' businesses. We've shaped a global ecosystem of consultants, industry professionals and alliance partners 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 deliver the solutions you need. Together, we help you deliver 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. AU3588

1510-1714390 MW
ED None

ey.com/giss

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means solving big, complex industry issues and capitalizing on opportunities to help deliver outcomes that grow, optimize and protect clients' businesses.

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

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

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

Our Risk Advisory Leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Scott Gelber	+44 207 951 6930	sgelber@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp