Insights on governance, risk and compliance

October 2014

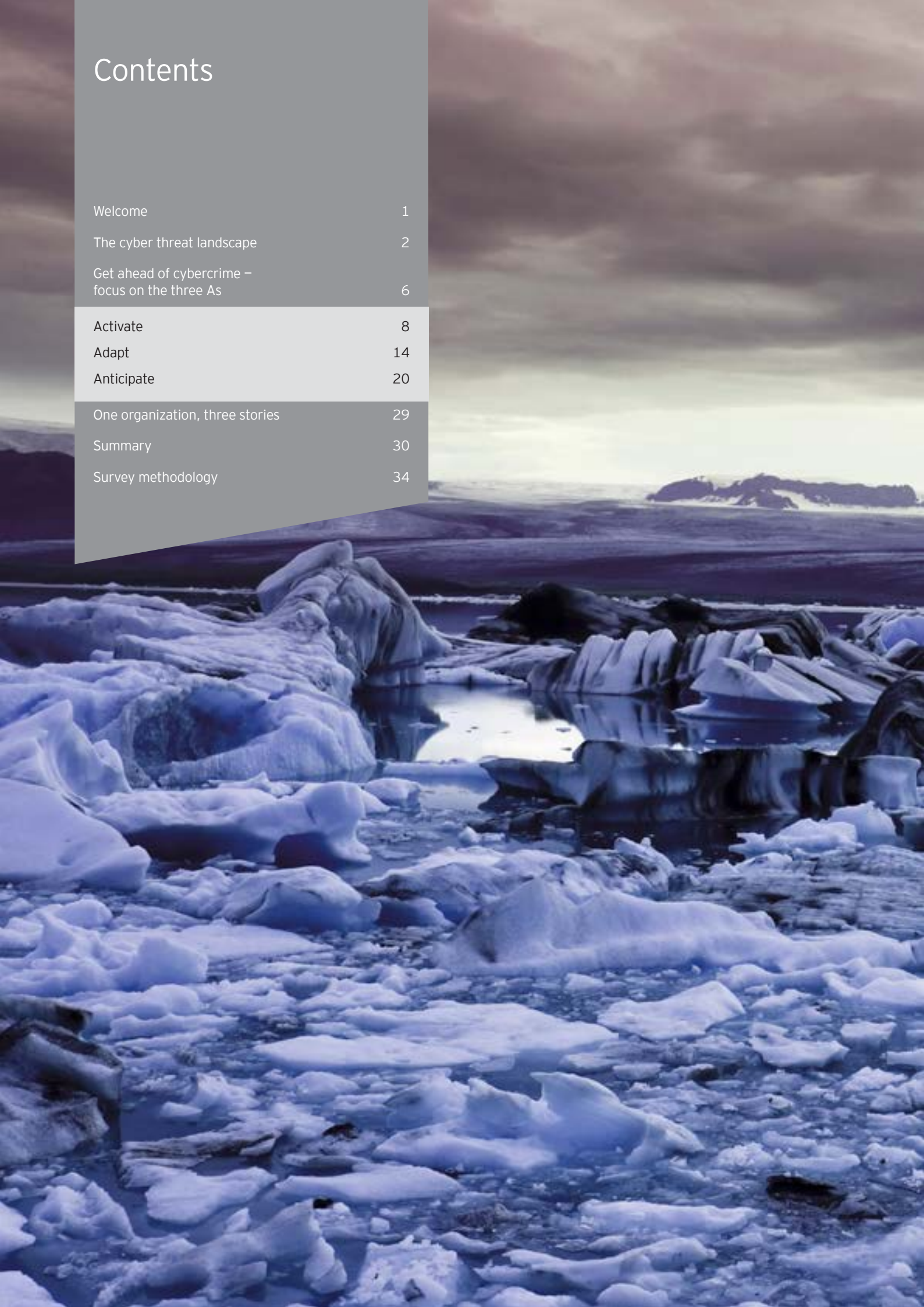
Get ahead of cybercrime

EY's Global Information Security Survey 2014

EY

Building a better working world

Contents



Welcome

Paul van Kessel
EY Global Risk Leader

Ken Allan
EY Global Cybersecurity Leader

Welcome to *Get ahead of cybercrime*.

"Anticipating cyber attacks is the only way to be ahead of cyber criminals." That's our message to businesses across the globe today, based on how 1,825 organizations responded to our 17th Global Information Security Survey (GISS), which this year focuses on how well organizations are managing cyber threats and what they need to do if they are to get ahead of today's cyber criminals.

Reports in the media regularly illustrate that cyber threats are increasing in their levels of persistence, sophistication and organization: the damage caused by a cyber attack can severely impact a business. As we discussed in the GISS 2013 report, even if you have not experienced an attack yet, you should assume that your organization will have been targeted, or that your security has already been breached.

In our 2014 survey, we discovered that organizations are making progress on building the foundations of cybersecurity – and this progress is important – however, most respondents report having only a "moderate" level of maturity in their foundations. There is still a lot to do.

The survey also tells us that more organizations are looking beyond the foundations in their approach to cybersecurity. These organizations are adapting their cybersecurity measures to changes in their business strategy and operations (for example, a merger, acquisition, introduction of a new product, entrance to new markets, implementation of new software) and to changes in the external business environment. But we know that they also need to change their way of thinking to stop being simply reactive to future threats.

Based on the above, we have organized this years' survey report to follow the cybersecurity journey:

- **Activate**
  This part of the report covers the foundations of cybersecurity. What is the status in 2014 and what are the most important elements that need more attention?
- **Adapt**
  Next we are going to focus on change. What are organizations doing to adapt their cybersecurity measures to the changing requirements? Can those organizations better defend themselves as cyber threats change and they integrate more advanced technologies?
- **Anticipate**
  The last part of the report will talk about how leading organizations can reach a state of readiness – to be confident in their assessment of risks and threats and prepared for what is coming. In other words: how to anticipate and get ahead of cybercrime.

By undertaking this journey, organizations will transform themselves from being an easy target into something more formidable. Eventually, they will – for the first time – be truly prepared for attacks.

We would like to extend a personal note of thanks to all of our survey participants. We appreciate the time they took to share their experiences with us. We welcome your reactions to this report.

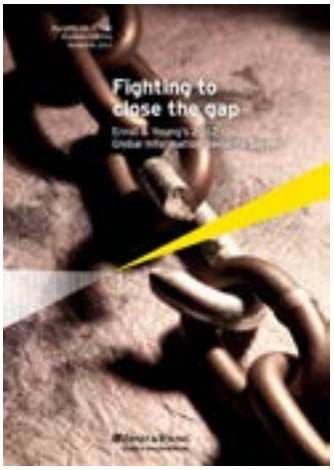
Every organization is at risk of a cyber attack, so let us continue this discussion together.

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

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

The cyber threat landscape

Global Information Security Survey 2013, *Under Cyber Attack*
www.ey.com/giss2013



Global Information Security Survey 2012, *Fighting to close the gap*
www.ey.com/giss2012

The disappearing perimeter

Cyber threats will continue to multiply. The advent of the digital world, and the inherent interconnectivity of people, devices and organizations, opens up a whole new playing field of vulnerabilities. In our Global Information Security Surveys of 2012 (*Fighting to close the gap*) and 2013 (*Under Cyber Attack*) we described this trend.

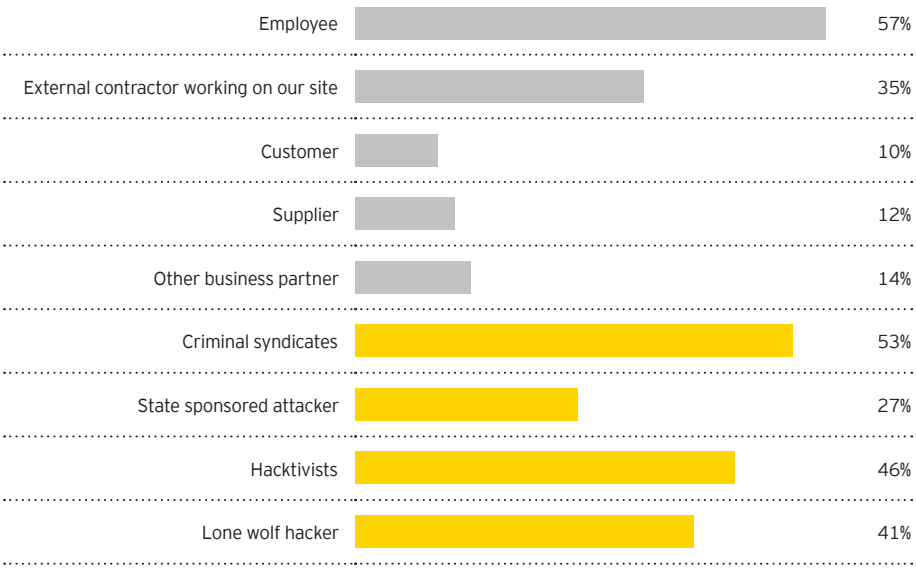
The short summary below highlights the top five reasons why effective cybersecurity is increasingly complex to deliver: they illustrate that the security defenses of organizations are under increasing pressure, further eroding the traditional perimeter and, in turn, creating more motivation for threat actors.

1	Change	In this post-economic-crisis world, businesses need to move fast. New product launches, mergers, acquisitions, market expansion, and introductions of new technology are all on the rise: these changes invariably have a complicating impact on the strength of an organization's cybersecurity.
2	Mobility and consumerization	The adoption of mobile computing resulted in blurring organizational boundaries, with IT getting closer to the user and further from the organization. The use of internet, smartphones and tablets (in combination with bring-your-own-device) has made organizations' data is accessible everywhere.
3	Ecosystem	We live and operate in an ecosystem of digitally connected entities, people and data, increasing the likelihood of exposure to cybercrime in both the work and home environment.
4	Cloud	Cloud-based services, and third party data management and storage, open up new channels of risk that previously did not exist.
5	Infrastructure	Traditionally closed operational technology systems are now being given IP addresses so that cyber threats are making their way out of the back-office systems and into critical infrastructures such as power generation and transportation systems, and other automation systems.

The growing attacking power of cyber criminals

The attacking power of criminals is increasing at an astonishing speed. Attackers have access to significant funding; they are more patient and sophisticated than ever before; and they are looking for vulnerabilities in the whole operating environment – including people and processes.

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



In our previous surveys, employees were seen as the most likely source of an attack. In this year's GISS, employees are still seen as a significant risk. However, for the first time, we found that when the different types of external attacker were combined (criminal syndicates, state sponsored attackers, hacktivists and lone wolf hackers) these threats were considered to be significantly more likely as a risk source. And nearly all our respondents have one or more external attackers included in their rating.

The roadblocks facing today's organizations

In the following sections of this report we will look at what organizations are doing to address these challenges, but first we need to consider what are the roadblocks that need to be removed before an organization can successfully get ahead of cybercrime.

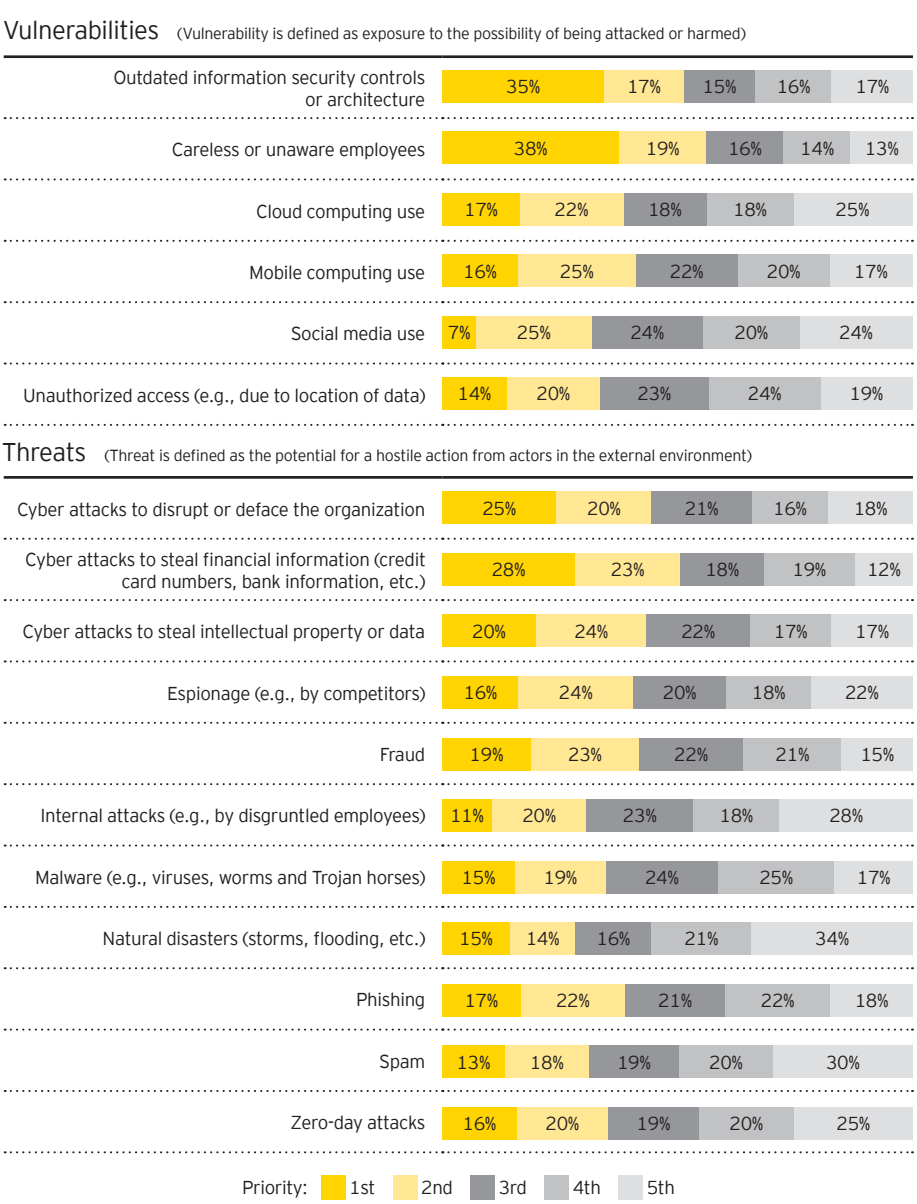
Roadblock 1 – Lack of agility

Not only are threats growing, our survey respondents also tell us that there are still known vulnerabilities in their cyber defenses. In other words, it is understood that there is a clear and present danger, but organizations are not moving fast enough to mitigate the known vulnerabilities – 37% tell us that they have no real time insight on cyber risks, and for a further 27% it is only "sometimes" available. As a result, organizations are lagging behind in establishing foundational cybersecurity. *See the "Activate" section to learn more about the areas requiring most attention, according to our survey.*

Breaking news!

Combined external attackers now significantly more likely as a risk source than internal threats.

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



43%

of respondents say that their organization's total information security budget will stay approximately the same in the coming 12 months and a further 5% said that their budget will actually decrease.

53%

of organizations say that lack of skilled resources is one of the main obstacles that challenge their information security.

Roadblock 2 – Lack of budget

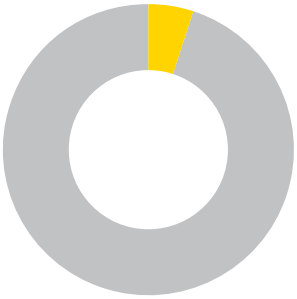
As we have seen before, the lack of budget is one of the most challenging roadblocks. In former years, we have been relatively positive about the difference between the available budget for cybersecurity and the amount of budget that was necessary, as we have seen a year-on-year increase of cybersecurity budgets. Now, for the first time, we see more organizations reporting that their budgets will remain flat.

Although we are experiencing ever greater attention on cybercrime in the boardroom and from non-executive directors around the globe, it seems that this interest doesn't translate into additional money. Nevertheless, there is still a need for more money and resources to face the growing threats effectively.

Roadblock 3 — Lack of cybersecurity skills

The most important roadblock is the lack of cybersecurity skills. While the need for specialists deepens, every year our survey shows that the lack of specialists is a constant and growing issue. Also there is the need to build skills in non-technical disciplines to integrate cybersecurity into the core business.

Sophisticated organizations not only defend themselves against cyber attacks; they use analytical intelligence to anticipate what could happen to them and have the confidence in their operating environment to know they are prepared (*see the "Anticipate" chapter for more information*). However, our survey points out that it is very difficult to hire the specialists necessary to perform the analysis on threat intelligence data, draw relevant and actionable conclusions, and enable decisions and responses to be taken.



5%

of organizations have a threat intelligence team with dedicated analysts and external advisors that evaluate information for credibility, relevance and exposure against threat actors.

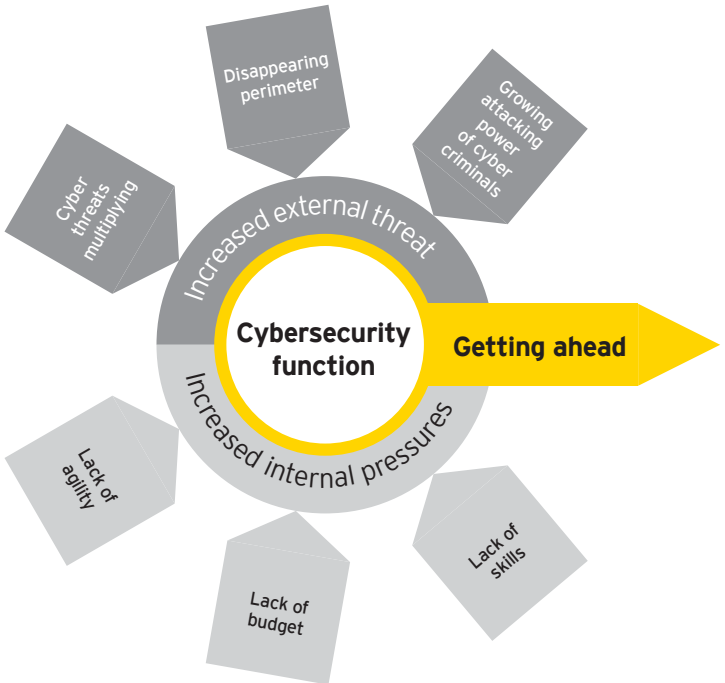
The growing threat to operational technology

The resilience of operational technology systems (OT systems, such as power generators, transportation systems, flight control systems and gas distribution systems) becomes more and more important and more and more challenging at the same time. New technologies, regulatory pressure and changing business requirements call for more cybersecurity. However, securing OT is not an easy task due to the complexities of the OT environments, legacy systems, different vendor architectures, and cultural differences between OT and IT teams.

Due to the relative ease of access via IP-addresses, OT systems are often targets for cyber criminals and should be included in an organization's approach to improving cyber maturity. Examples of attacks have included:

- Infection by a worm virus of process control systems that ran a railway network, causing the unreliable usage of the railway tracks
- Access to a bank's facility management system and manipulation of the building's internal air conditioning system that caused servers to shut down due to over-heating
- Malware that destroyed the controls systems of a nuclear power plant, or process controls over the upstream installation of an oil and gas company

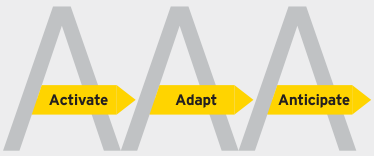
Looking at what we have discussed so far (*summarized in this diagram*), we have seen that there is a rapidly expanding threat landscape, the power of cyber criminals is growing, and organizations are still struggling with a number of roadblocks. We know that it is not easy to get ahead of cybercrime.



Get ahead of cybercrime –

In the following chapters we will discuss three different stages of the journey to cybersecurity maturity – Activate, Adapt and Anticipate (the three As) – which need to be executed in a tight sequence (and consistently recurring) to deliver state-of-the-art cybersecurity.

We have found that organizations' responses to cybercrime fall into three distinct stages, and the aim should be to implement ever more advanced cybersecurity measures at each stage.



Activate

Organizations need to have a solid foundation of cybersecurity. This comprises a comprehensive set of information security measures which will provide basic (but not good) defense against cyber attacks. At this stage, organizations establish their fundamentals – i.e., they "activate" their cybersecurity.

Foundational

Bolt-on cybersecurity

A focus on safeguarding the **current** environment

A **static** approach

Where am I?	*Check the boxes below and identify how many of the characteristics of your organization meet the Activate profile.*
Incident management	☐ Never had an incident ☐ Third party releases information publicly or notifies you ☐ Unsure who would respond ☐ No single person nominated to disclose information publicly ☐ No incident response plan
Leadership discussions	☐ Not a boardroom issue ☐ Leadership conversations focus on tools and policies ☐ Business not engaged as security leadership team
Metrics	☐ Headcount ☐ Maturity models ☐ Budget ☐ Compliance

- focus on the three As

Adapt

Organizations change – whether for survival or for growth. Threats also change. Therefore, the foundation of information security measures must adapt to keep pace and match the changing business requirements and dynamics otherwise they will become less and less effective over time. At this stage, organizations work to keep their cybersecurity up-to-date; i.e., they 'adapt' to changing requirements.

Anticipate

Organizations need to develop tactics to detect and detract potential cyber attacks. They must know exactly what they need to protect (their 'crown jewels'), and rehearse appropriate responses to likely attack/incident scenarios (including accidents): this requires a mature cyber threat intelligence capability, a robust risk assessment methodology, an experienced incident response mechanism, and an informed organization. At this stage, organizations are more confident about their ability to handle more predictable threats and unexpected attacks; i.e., they 'anticipate' cyber attacks.

Dynamic	**Proactive**
Built-in cybersecurity	**Built-beyond** cybersecurity
A focus on the **changing** environment	A focus on the **future** environment
A **dynamic** approach	A **proactive** approach
Check the boxes below and identify how many of the characteristics of your organization meet the Adapt profile.	*Check the boxes below and identify how many of the characteristics of your organization meet the Anticipate profile.*
☐ Organization identifies and reacts to its own incidents ☐ Incident response plan notifications of participation ☐ Incident response teams include IT leadership ☐ Public relations established ☐ Acceptance a breach will occur, or has already occurred	☐ Organization prepares for oncoming breaches based on threat scenarios ☐ Corporate senior leadership is part of response team ☐ External communication is controlled and fact-based defensible positions
☐ Disaster recovery plans ☐ Regulatory landscape and impacts ☐ IT leadership and business leaders discuss reality of breach occurrence and impact	☐ Standing boardroom agenda item ☐ IT leadership and business leaders discuss how security enhances business ☐ Leadership level cooperation with peers
☐ Attacks/incidents ☐ Revenue impact of breach ☐ Advanced risk analysis and scoring	☐ Revenue support/growth/protection from security ☐ Alignment to business objectives

Establish foundations

Every organization needs a solid foundation of cybersecurity. Putting this foundation in place is not an easy task and the specifics of exactly what is needed will depend on industry sector and geography.

This is not new: in our Global Information Security Survey report of 2012 (*Fighting to close the gap*) we explored the gap between the actual cybersecurity measures taken and the necessary foundational cybersecurity components that should be in place. This foundation provides the first step in the cybersecurity journey.

Activate

Organizations that have activated the foundations for cybersecurity but not moved beyond this will typically display the following three shortfalls in their capabilities, demonstrating why the journey must continue.

1. **Bolt-on cybersecurity**
   The organization's cybersecurity has been added on to business processes and activities. It has not yet been integrated into the business, it is not seen as an added-value activity and is viewed as a cost factor which needs to be limited as much as possible. If application development is all about security certification approval after development or at major gates, the organization is stuck here ... with bolt-on security.

2. **A focus on safeguarding the current environment**
   This foundation level for cybersecurity starts with looking at the risks the organization is already aware of based on prior experience; the goal is to make sure the measures are in place that will solve any weaknesses. If conversations are just around risk assessments, controls efficiency and risk mitigation, the organization remains in the Activate level.

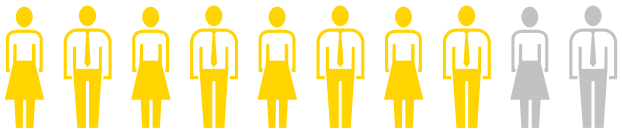
3. **A static approach**
   This level of cybersecurity capability is aimed at enabling the business to carry out its known and regular day-to-day functions securely. The organization will be rule-based and compliance-driven, relying on metric-driven reporting – it can only deal with threats in a world without change.

All businesses, no matter how advanced in their cybersecurity development, must achieve mastery of the foundational requirements of cybersecurity. However, our observation based on this year's survey is that too many organizations do not even have all foundational components of cybersecurity in place.

In this report we have focused on five critical areas, as this year's survey, and EY's experience from working with our global clients, has shown that this is where the biggest issues can arise:

- Executive buy-in
- Resources
- Performance
- Access to data
- Cost vs. value

Component	What are the issues?
Executive buy-in	▸ Leadership on cybersecurity strategy, plan and execution comes from lower organizational levels or is seen as an IT issue. ▸ There is not a consistent threat management system in place; threats are not regularly discussed in the boardroom.
Resources	▸ Cybersecurity tasks are not adequately resourced and/or performed by skilled people. ▸ Cybersecurity teams do not have visibility and knowledge about attacks.
Performance	▸ Many organizations are spread too thin: they maintain too many cyber capabilities and – as a result – with moderate effectiveness. ▸ The effectiveness of cybersecurity is not measured.
Access to data	▸ Employees are a risk to cybersecurity, and their Identity and Access management (IAM) program is weak. ▸ Excessive manual processing and irregular reviews or reports make it too easy for employees to have inappropriate access to data. ▸ Movers, leavers and joiners are a key cyber risk area.
Cost vs. value	▸ Too many organizations view the costs of cybersecurity as considerable. ▸ Organizations do not appreciate the benefits of the measures they already have. ▸ Organizations significantly underestimate the potential cost of a cyber attack.

Survey findings	Implications
 Nearly 80% of CIOs or IT departments have the Information Security function reporting directly to them, compared with just 14% reporting directly to the CEO.	▸ Organizations need to involve senior leadership in cybersecurity. ▸ Lack of executive buy-in opens the doors to mistakes and cyber criminals; cybersecurity will miss the necessary direction and investments.
 Fewer than 20% of organizations have real time insight on cyber risks readily available.  20% have published sources of cyber attacks on their sector peers readily available.	▸ Cyber threats are overlooked or the response is too late. ▸ Cyber criminals successful use of phishing is a result of a lack of security awareness.
 Across almost every cybersecurity process between 35% and 45% of respondents rated themselves "still a lot to improve."	▸ Foundational cybersecurity processes are not working properly, leaving a broad range of options for those performing an advanced persistent threat (APT).
 Nearly two thirds of organizations do not have well-defined and automated IAM programs.	▸ We have seen that employees are seen as a huge threat for cybersecurity; while organizations are looking for hackers coming in from the outside, fraud is already happening from the inside.
 63% cite budget constraints as the main obstacle to making a contribution and delivering value.  Nearly 50% will see no increase in budget over the coming 12 months.	▸ Organizations must understand they are under daily attack, the attackers show no signs of giving up, they are getting smarter and more targeted. The next breach could be fatal.

Foundational activities all organizations need to "activate"

Organizations that have not yet reached the foundational level of cybersecurity need to act fast. To help them, here are six of the most frequently overlooked yet critical actions to be considered urgently:

1. **Security assessment and roadmap**
   Conduct a cyber threat assessment, current state maturity assessment, target state definition, gap analysis and design of implementation roadmap, alignment with leading practices such as ISO 27001.
2. **Get Board-level support for a security transformation**
   Redefine cybersecurity governance, e.g., realigning cybersecurity outside of the IT function and ensure that the Board understand processes.
3. **Review and update security policies, procedures and supporting standards**
   Implement an information security management system (ISMS)
4. **Establish a Security Operations Center (SOC)**
   Develop monitoring of known cases and incident response procedures.
5. **Design and implement cybersecurity controls.**
   Assess the effectiveness of data loss prevention processes and IAM. Harden the security of IT assets, such as servers and firewalls, network components and databases.
6. **Test business continuity plans and incident response procedures**
   Instigate regular penetration testing of the network perimeter, ingress points and software applications; and identify exploitable weaknesses.

The Security Operations Center

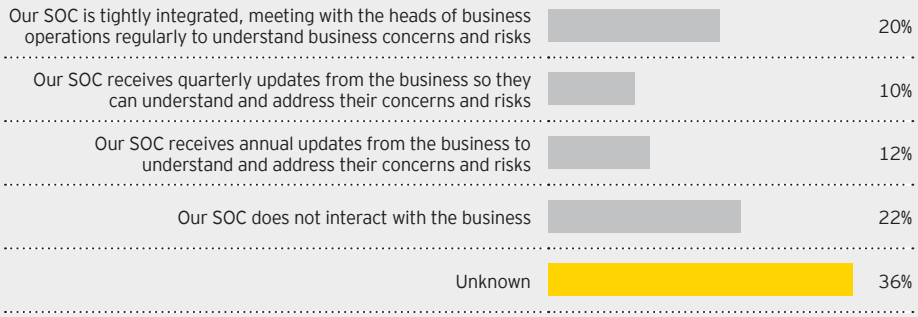
Vital to foundational cybersecurity are the processes and technology that support the Information Security function. These are most effective when they are centralized, structured and coordinated, which is why a Security Operations Center (SOC) is a valuable starting point. While a SOC can be outsourced, it is important to ensure that it meets the needs of your business operations – we are seeing a clear shift from a "one size fits all" into a bespoke SOC situation – and that its knowledge of cybersecurity threats and issues is up to date and aligned to the business strategy.

It is concerning that over 40% of organizations in our survey do not have a SOC. For those that do, the benefits of centralization are either not being met or are not communicated or understood by organizations. Over half of respondents were either unable to answer the question about how well the SOC met business operations' needs, or declared that it was unknown, or that the SOC didn't interact with the business.

42%

of organizations do not have a SOC.

How does your SOC ensure they are meeting the needs of business operations?

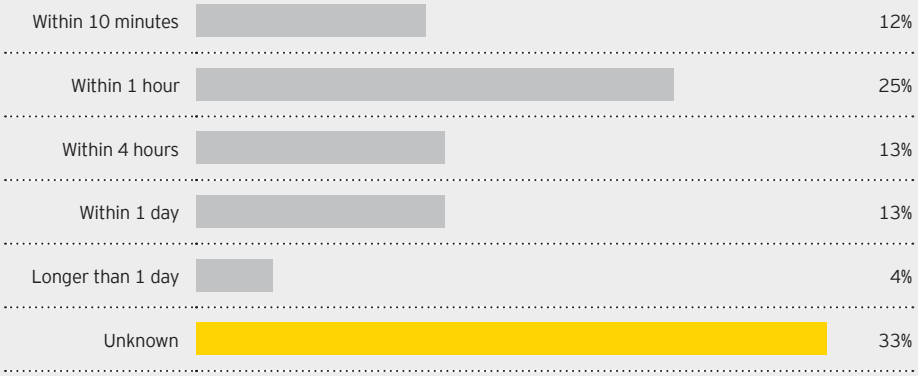


There is similar lack of awareness in the area of how the SOC stays up to date with the latest threats. Over 50% of respondents either could not answer the question, or did not know how long the SOC would take to initiate an investigation on a discovered or alerted incident. Before any improvements can be requested or mandated, organizations first need to be better informed about what their SOC does.

37%

say that real time insight on cyber risk is not available.

How long on average does it take for your SOC to initiate an investigation on discovered/alerted incidents?



Overall, the technology infrastructure and endpoints of the SOC need to be improved. If more of the benefits of a SOC were being realized, then the general ability of an organization to protect itself in even the most basic functions would start to deliver benefits.

Take a dynamic approach

Organizations that have established the foundation of cybersecurity have commenced the journey, but to remain competitive, a business must constantly change and adapt to a changing business environment and to the evolving threats that come along with those changes. As a result, the organizations' cybersecurity requirements will need to change as well — changing the control infrastructure and technology capability/usage to support the improved situational awareness of known risks. If an organization doesn't adapt, its cybersecurity foundation will quickly be obsolete.

Adapt

The Adapt stage adds the following features to the Activate level:

1. **Built-in security**
   Cybersecurity is considered and involved in everything the organization does: whether that is the development of a new business process, opening a new plant, an acquisition or the introduction of a new product. Changes in the business are immediately assessed from a cybersecurity perspective (it is not an afterthought) and changing cybersecurity requirements are built in to all business processes. As a result, cybersecurity will be up-to-date continuously.

2. **A focus on the changing environment**
   A more mature cybersecurity continuously adapts to ongoing changes in the business and its environment. For instance: Going digital or using cloud services can introduce risks the organization was not facing before. Increased situational awareness enables the risk assessment to incorporate internal changes, and to be able to react to expected changes in the threat landscape.

3. **A dynamic approach**
   The organization's cybersecurity is flexible, agile and under constant revision. It continually adapts to better protect the business.

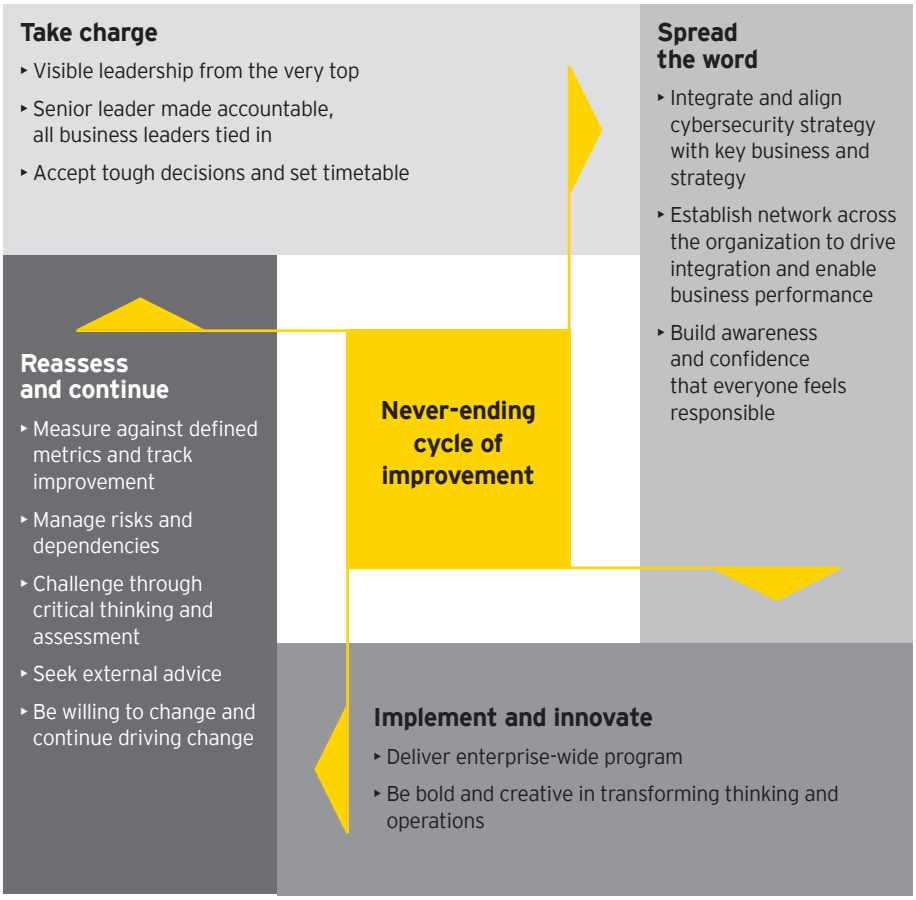
Cycle of improvement: the approach to adaptability

Organizations are undergoing constant change. Here are a number of examples:

- The necessity to integrate new technologies (social media, cloud, digital, big data, etc.) into business processes
- The exponential rise of mobile devices (BYOD, etc.), blurring the lines between the business and personal world
- The growth in managed services and remote hosting, with greater reliance on complex apps (many hosted remotely)
- The integration of process control infrastructure with the back office and the outside world
- Rapidly changing regulatory environment and requirements

As a result, organizations have to cope with a never-ending cycle of new threats and challenges requiring the adoption of a never-ending cycle of improvement and re-evaluation of the changing cybersecurity capabilities. Organizations need to establish a system that enables them to manage this cycle in an efficient and effective manner so that they benefit from embracing new/different security opportunities which, in turn, enable the business and save costs.

The improvement cycle



Running backwards to grasp reality

In order to get ahead of cybercrime, it is essential to keep your cybersecurity measures 100% aligned with your business. This challenge has been high on the agenda for several years, and improvement has been made year on year. However, for the first time in five years, the GISS survey shows us that organizations are effectively going backwards. Organizations are continuing to improve their cybersecurity, but the changes in the threat landscape (*see chapter 1 of this report*) are travelling at an even faster rate. We predicted this trend two years ago.* This also indicates that organizations are becoming more aware of the reality of threats – from the news or personal experience.

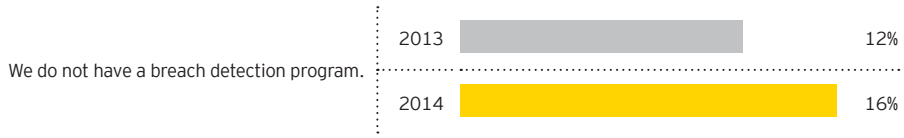
This year, our GISS found that:

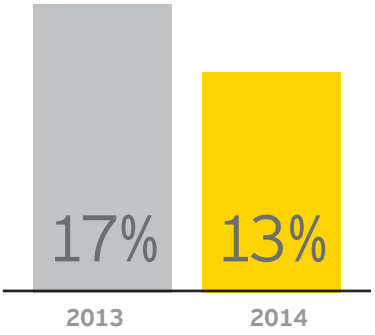
- 13% of respondents report that their Information Security function fully meets their organization's needs – this is down from 17% in 2013.**
- Last year, 68% of respondents felt that their "Information Security function partly meets their needs and that improvement is under way." This has fallen to 63% this year.

These results show that organizations need to get more serious about cybersecurity. Using the improvement cycle described opposite will help them get back on track.

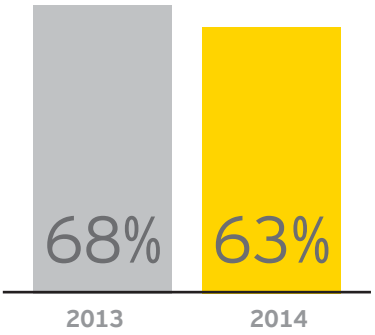
Our survey also explored why cybersecurity measures are not meeting the needs of so many organizations, for example in breach detection:

What statement best describes the maturity of your breach detection program?





Instead of an expected increase in the number of organizations reporting that their Information Security function fully meets the needs of their organization, our survey found a decrease.



Instead of an increase in the number of organizations reporting that their Information Security function partially meets their needs and that improvements are under way, there has been a decrease of 5%.

How to make vital improvements

So what are the areas that need specific and more attention? What "low hanging fruit" would allow organizations to make progress easily?

Here are four areas of improvement (applicable for most organizations):

1. Improve the Security Operations Center (SOC)

A well functioning SOC is an important asset to get ahead of cybercrime. If there is one security function in the organization that should be aware of the latest threats, it is the SOC. Broadly, only a third of respondents felt that their SOC was keeping up to date with the latest threats – this is an alarming result.

One of the root causes is that – in most cases – SOCs are overly focused on the technology. Although the features of the technology are important (what can be measured and monitored), the starting point should be the business (what needs to be measured and monitored).

Interaction with the business is key: 22% of GISS respondents tell us that there is no interaction between the SOC and the business – and a further 36% did not know. How can a SOC focus on the right risks (and changing risks) if the business is not connected to the SOC on a regular basis?

*See EY's Global Information Security Survey 2012 – *Fighting to close the gap (www.ey.com/giss2012)*

**EY's Global Information Security Survey 2013 – *Under cyber attack (www.ey.com/giss2013)*

55%

of organizations do not include information security in employee performance evaluations.

2. Create a core cybersecurity team

Consolidate cybersecurity approaches and activities around a core team: by establishing the cybersecurity knowledge in a core team, organizations will be able to adapt to new threats more easily. This core team can be organized centrally or distributed across functions/borders depending on the size and the requirements of the organization.

The core team should also focus on training, skills and awareness, and make the practice of information security part of everyday life for every employee – the members of the core team should act as ambassadors who practice what they preach.

3. Establish accountability

Greater accountability and performance measurement are key ways to achieve behavior change. If employees understood that their own job security was under threat because the security of the organization was under threat, and that cybersecurity was a performance metric, this could encourage a permanent change in awareness and behavior. Embed the required behaviors into employee contracts – especially for those with access to critical information – and include it in their performance evaluations. Breaches of information security protocols (even if there were no significant consequences) should be taken very seriously.

In addition to informing employees about cyber threats, find ways to make them the "eyes and ears" of the organization and ensure there is a clear escalation process everyone can follow in the event of an employee noticing something suspicious. In our survey, forensics support and social media are the lowest ranked areas on information security priority, yet these techniques and channels can be the first way of spotting that the organization is at risk of an attack.

4. Go beyond the borders

With a transformation cycle in place, organizations can start to look beyond their own borders, and begin to assess the impact of a cyber attack on their business partners, suppliers, vendors – a community that can be described as their business "ecosystem" (*see page 19*). Their own effective transformation will have revealed leading practices, and now these practices can be communicated to the ecosystem so that suppliers and vendors could be contractually obliged to conform.

Take action to improve and transform

If your organization is between the Activate and the Adapt levels, here are five steps you should be considering urgently:

1. Design and implement a transformation program
Support a step improvement in cybersecurity maturity over and above the basic level where security projects are delivered separately in a piecemeal fashion. Get external help in designing the program, and providing program management.

2. Decide what to keep in-house and what to outsource
For example, decide whether to keep a core team in your own SOC providing full in-house capability, or outsource to a managed security services provider (MSSP), or move to a blended model.

3. Define a RACI matrix for cybersecurity

4. Define the organization's ecosystem
Consider the knock-on impact of security breaches on your third parties, and make moves to eliminate or lessen potential security gaps in your interaction with them.

5. Introduce cybersecurity awareness training for employees
Perform a maturity assessment, target state definition, and gap analysis. Develop and implement a training plan for staff (including contractors).

Looking beyond borders: the business ecosystem

Our research shows that in the battle against cybercrime most companies spend the majority of their time and resources building a fence around their internal organization – including their data, systems and personnel. This is a starting point, but the perimeter is no longer stable, and a fence no longer possible.

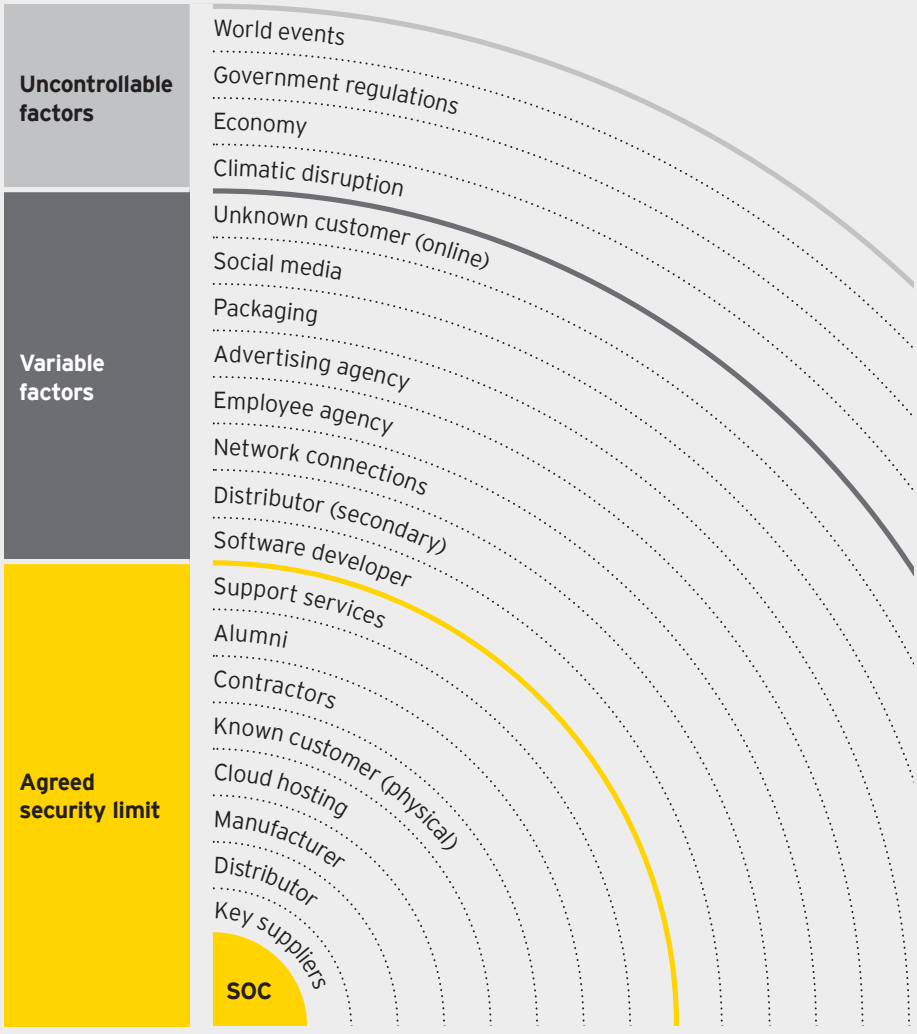
Most of today's business is done outside the defensive fence. In order for organizations to be able to communicate with their business partners, they must create "holes" in the fence. As a result a cybersecurity system should also include the broader network, including: clients, customers, suppliers/vendors, business partners and even their alumni – together called "the business ecosystem."

For an organization to be able to effectively manage the risks in its ecosystem, it needs to clearly define the limits of that ecosystem. It also needs to decide what it is willing to manage within those boundaries: is it just the risks faced by groups that are one step from the organization itself (e.g., suppliers); or should the organization also try to influence the mitigation of risks faced by groups that are two steps from the center (e.g., the suppliers of suppliers)?

Organizations need to ask:

- What is our "security limit;" in other words: with how many partners should we work with to enhance overall cybersecurity?
- How much can we do to manage the risk in the business ecosystem?
- Are we prepared to accept a certain level of risk from the business ecosystem?

Your business ecosystem



Be in a proactive state of readiness

There is only so much an organization can do to respond to threats that have already arisen. But an organization that can only react to new threats once they have become active may well find out that it has acted too late.

The only way to get ahead in this complex and dynamic environment is to grasp the challenges head on – embrace cybersecurity as a core aspect of the business, and as an integral capability to survive and thrive. Becoming successful and staying successful is a never-ending journey, and building and maintaining the organization's cybersecurity capability is part of this.

The ambition should be to move to a state of readiness – to be able to anticipate what is likely to happen and to prepare, act and respond accordingly. To do this means shedding the "victim" mindset of operating in a perpetual state of uncertainty (and anxiety) about unknown cyber threats, leaving the organization open to unpleasant and damaging surprises. It means building awareness and advanced capabilities, developing a compelling strategy and installing cybersecurity components throughout the business: it means promoting confidence in the organization's ability to deal with cybercrime.

Anticipate

To be at the Anticipate stage, the following characteristics need to be added:

1. Built-beyond security

- **Be alert, ready to act and respond quickly, in a balanced manner.** Leadership accepts cyber threats/risks as a core business issue, and cybersecurity capabilities are part of a dynamic decision process. This enables preventative action and response mechanisms to operate smoothly and quickly.
- **Know your "crown jewels."** The organization cannot be ready for attacks if it does not know the assets most valuable to the business. It must be able to prioritize these assets and understand the impact of them being breached, compromised or made unavailable in any way; then link this into the threat assessment process.

2. A focus on the future environment

- **Know your environment, inside and out.** Comprehensive, yet targeted, situational awareness is critical to understanding the wider threat landscape and how it relates to the organization. Cyber threat intelligence can bring this knowledge — it incorporates both external and internal sources of risk, and covers both the present and future, while learning from the past.
- **Continually learn and evolve.** Nothing is static — not the criminals, not the organization or any part of its operating environment — therefore the cycle of continual improvement remains. Become a learning organization: study data (including forensics); maintain and explore new collaborative relationships; refresh the strategy regularly and evolve cybersecurity capabilities.

3. A proactive approach

- **Be confident in your incident response and crisis response mechanisms.** Organizations that are in a state of anticipation regularly rehearse their incident response capabilities. This includes war gaming and table top exercises, through to enacting complex incident scenarios that really test the organization's capabilities.

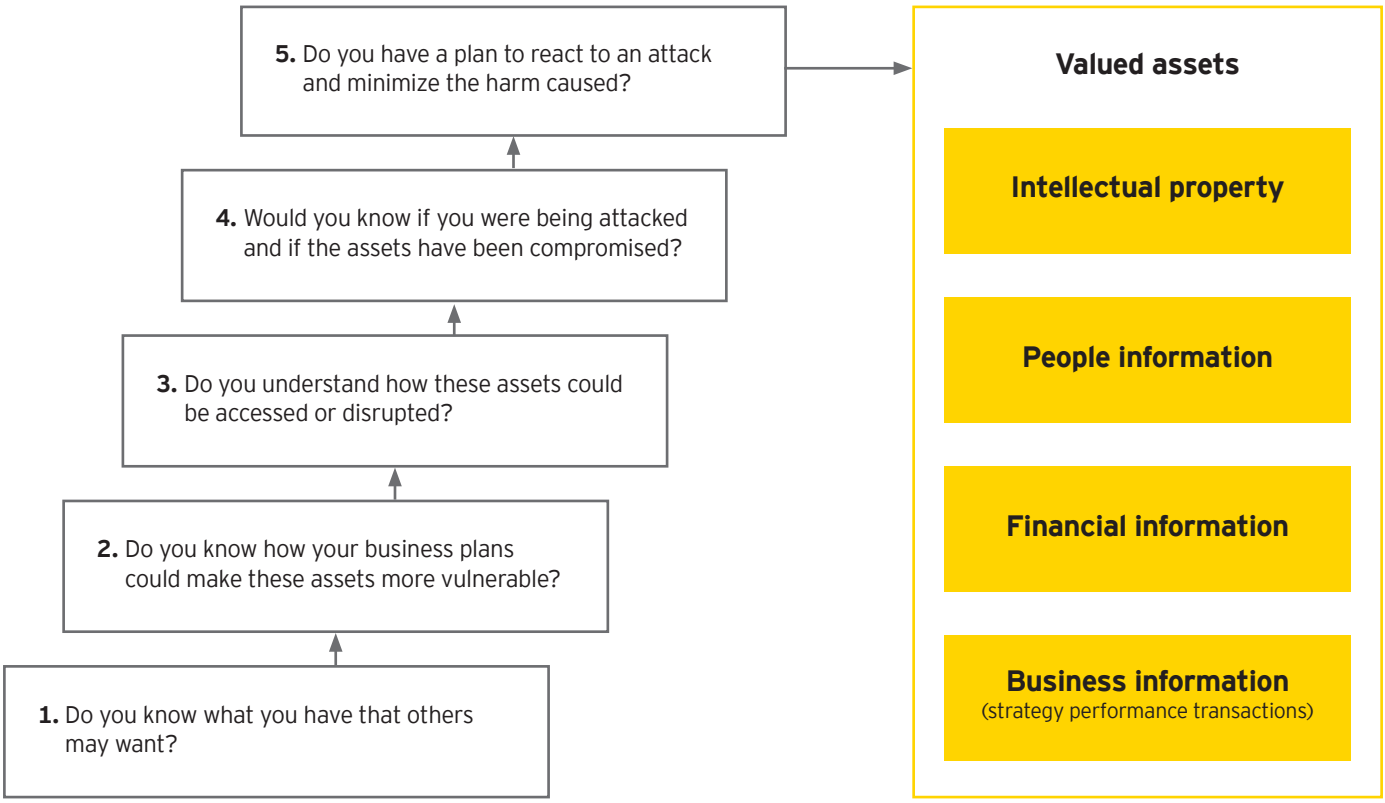
Get ready to anticipate

An organization in a state of readiness inhabits an entirely different mindset, sees the world differently and responds in a way the cyber criminals would not expect. It requires behaviors that are thoughtful, considered and collaborative. It learns, prepares and rehearses. No organization or government can ever predict or prevent all (or even most) attacks; but they can reduce their attractiveness as a target, increase their resilience, and limit damage from any given attack.

Learning how to stay ahead is challenging and takes time, but the benefits for the organization are considerable. The organization will be able to exploit the opportunities offered by the digital world, while minimizing exposure to risks and the cost of dealing with them.

To start, an organization and its leadership must know answers to all of these questions to be confident. If any of the answers is "no," that is where to focus and where changes need to be made.

Being attacked is unavoidable, so how prepared are you? Can you answer "yes" to these five key questions?



The following sections outline what an organization can do to get ahead, and enable it to answer "yes" to everything above and move beyond.

Understand your threat environment and establish early detection

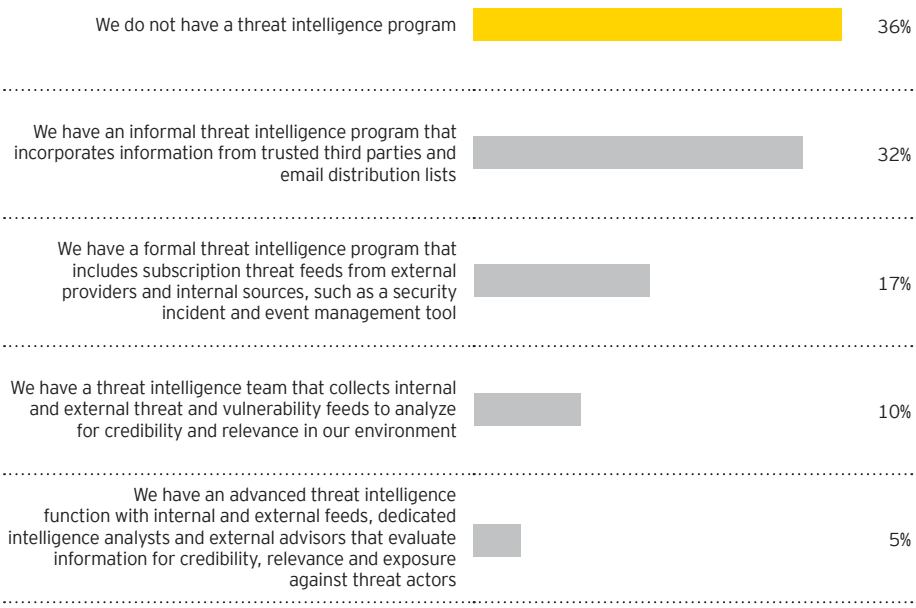
It is not enough to just know there are threats. The organization needs to understand the nature of those threats and how (and where) these might manifest themselves, and assess what the impact would be. Early warning and detection of breaches is key to being in a state of readiness. However, the majority of organizations are only able to detect fairly simple attacks, meaning they may not know they have already been breached by a more sophisticated attack and they will not be able to detect future attacks of this nature.

Incorporating or establishing a cyber threat intelligence capability can help get the organization ahead of cybercrime. At a tactical level, this capability will sit in the SOC, but the reach of this function will extend into the strategic level and the C-suite, if done well.

- What is happening out there that the organization can learn from?
- How can the organization become "target hardened" and is this required?
- How are other organizations dealing with specific threats and attacks?
- How can the organization help others deal with these threats and attacks?
- Does the organization understand the difference between a targeted attack and a "random" one?
- Which threat actors are relevant?

All these questions can be answered through cyber threat intelligence, but our survey indicates that few organizations have a grasp of what that is and what it can deliver:

Which statement best describes the maturity of your threat intelligence program?



56%

of organizations say that it is unlikely or highly unlikely that their organization would be able to detect a sophisticated attack.

36%

of respondents do not have a threat intelligence program.

Intelligence is about much more than just collecting information. The intelligence cycle comprises a sequence of activities:

1. Determine intelligence requirements

What does the organization need to be aware of? Where are the gaps in knowledge?

2. Collect information

Various open source feeds are available for external information, and there are many data feeds from internal systems.

3. Analyze and assess gathered information to produce an intelligence report

This can be sourced externally, or conducted internally. An understanding of the core business is crucial for any assessment to be meaningful.

4. Distribute and communicate the report

5. Take appropriate action

For cyber threat intelligence to be effective, this cycle will need to be performed quickly. Some activities can be automated, and techniques, tools and services are available for this. Other elements cannot be automated, and will require human involvement and intervention. There are a variety of cyber threat intelligence services available, and these will need to be evaluated specifically for the organization's requirements, appetite and maturity. However, the flaw of many of these services is that they flood the organization with information that is not meaningful or actionable, and often end up being ignored.

Cyber threat intelligence can also prove to be very useful in creating more value in risk management by pointing out potential flaws in the current network and ecosystem, which should result in process changes that would allow the organization to be more agile: decisions would be made faster; data would be protected; gaps would be uncovered, prioritized and mitigated. A solid threat intelligence program can also be further unlocked with a good metrics program and analytics, often tied into a company's Big Data program.

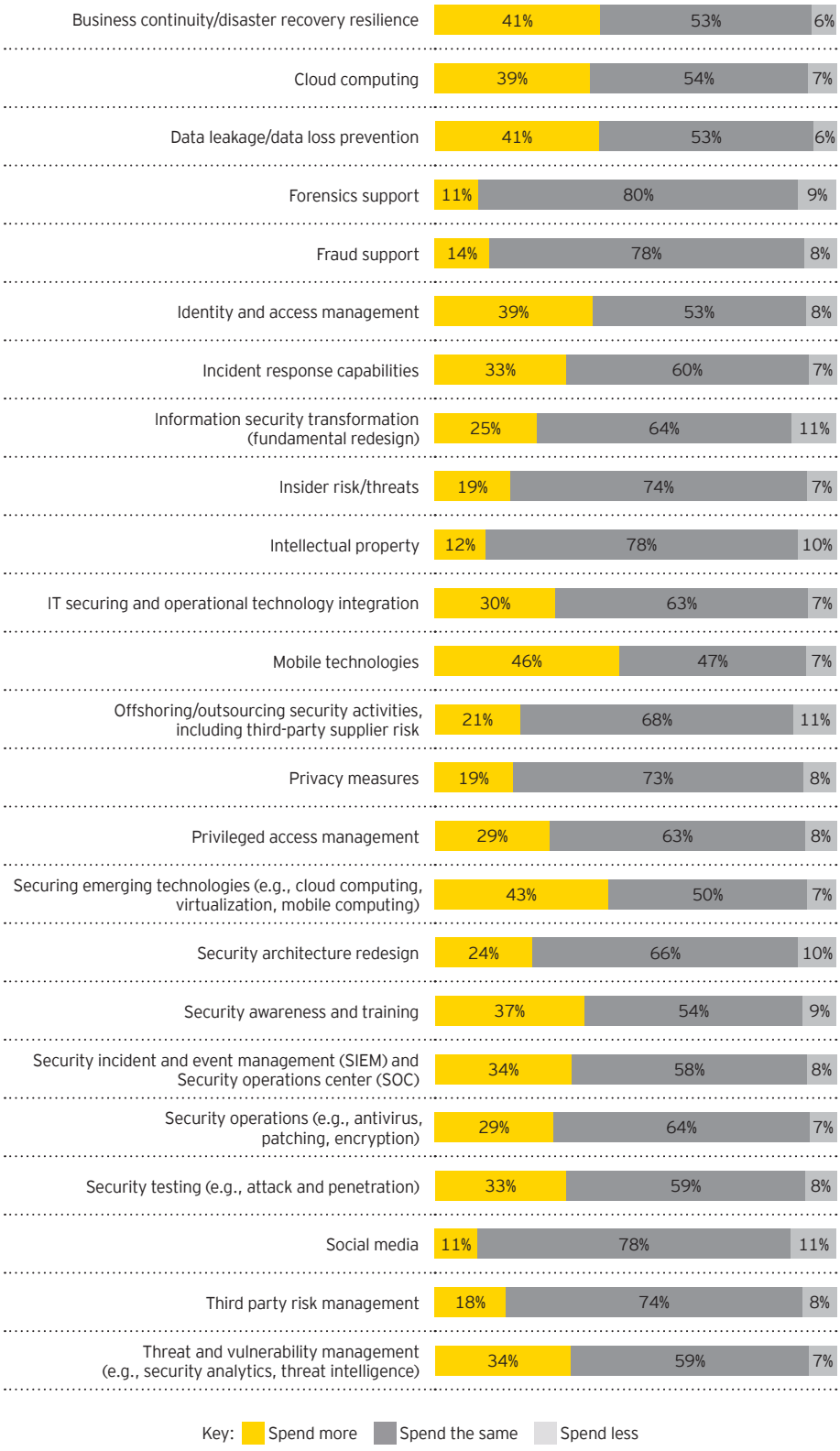
23%

of respondents state that their information security strategy outlines the future state of information security three to five years out.

Take a view of the past, present and future

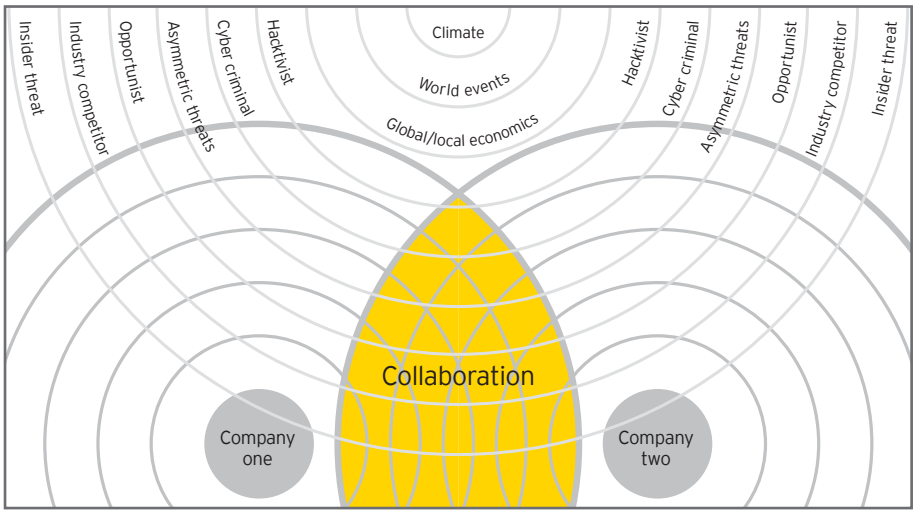
The organization's ambition needs to encompass efforts to look into the future, as well as learning from the past and being prepared for the now. Organizations should be kept informed of new/different trends in attack types and in the methods, tools and techniques to deal with them. It's vital to be kept informed about emerging technologies, and to keep exploring the opportunities for the business to exploit these, while keeping a firm eye on the new risks and weaknesses they may introduce. Our 2014 survey, however, shows that most organizations are still preoccupied with their current state and are not looking to the future:

Compared to the previous year, does your organization plan to spend more, less or relatively the same amount over the coming year for the following activities?



Get involved and collaborate

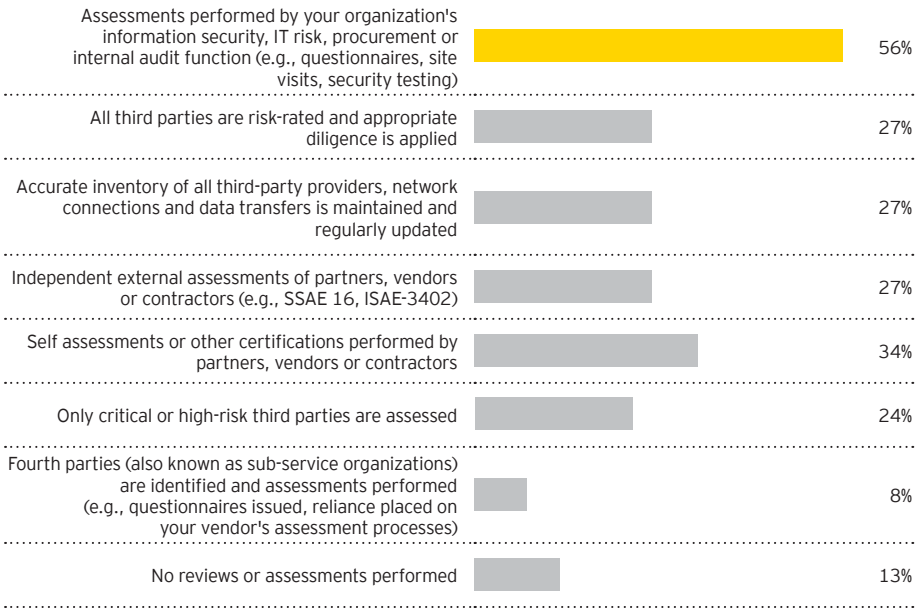
Collaboration is necessary at the Anticipate level. All organizations (and indeed individuals) are facing these challenges and, as capability matures, organizations are learning that collaboration bears fruit, especially if done in a targeted fashion. The sharing of information across a business ecosystem in a larger group (whether ad-hoc, semi-formal, or a moderated formal environment), is the secret ingredient for organizations that have the most success at understanding, scoping and mitigating intrusions in their networks.



This central collaborative component is also true of cyber threat intelligence. Information and intelligence sharing platforms exist in many forms (industry specific, cross-industry, government-run, linked to the national CERT, or standalone entities with government involvement, etc.); and governments and major organizations have started to take a leading role in establishing the policy and practice frameworks that support the development of resilient cyber ecosystems, e.g., US-CERT's Cyber Resilience Review (CRR) and the World Economic Forum's Partnering for Cyber Resilience (PCR) initiative. These forums will push time critical information to the organization, and also provide access to strategic insights on threat actors and future scenarios, mitigation techniques, industry context and government actions.

Collaboration also provides the organization with greater awareness of its partners and supply chain, and the ability to influence and learn from the whole ecosystem. Larger organizations need to understand that their security capabilities are often far more mature than those of some of their suppliers, so knowledge-sharing around cybersecurity, or coordinating cybersecurity activities with suppliers can be much more effective than going it alone. A shared solution tightens the protective layers in and around your ecosystem. However, it would require an organization to develop a "trust model," based around authentication, assurance agreements, etc. Any incident response exercises should include third parties and other players in your wider ecosystem.

How do you ensure that your external partners, vendors or contractors are protecting your organization's information?



Cyber economics

Organizations are using these four questions to assess the impact of a cyber attack in real-world terms, to understand the impact on the bottom line and the organization's brand and reputation.

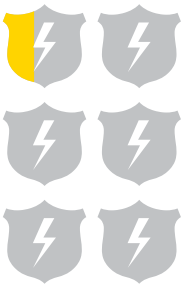
- How would the share price be affected?
- Would customers be impacted?
- Will this translate into reduced revenues?
- What will the costs be of having to repair damage to all internal systems and/or replace hardware because the organization was not prepared for an attack?

Cyber economic techniques are being developed to help organizations convert this into tangible figures.

Conduct cyber incident exercises

Is the organization confident that everyone knows what to do if an attack takes place? If not, then the damage from the attack will be far greater than expected.

Poor handling of cyber incidents have led to harsh impacts on many companies. Once a breach is detected, then having thorough knowledge of your critical assets and associated ramifications will allow the organization to set in motion the appropriate handling mechanisms. Stakeholders, customers, employees, PR, regulators – all these parties play a part in determining how well your organization weathers an attack.



6%

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.

58%

of organizations do not have a role or department focused on emerging technologies and their impact on information security.

Being in a state of readiness requires that the organization will have already rehearsed many different attack scenarios. At least once a year, the organization should rehearse its crisis response mechanisms through complex cyber attack scenarios. Different services are available to help the organization safely, but realistically, exercise in this fashion. It will be difficult, but the lessons learned will prove invaluable. Regulators in some areas are now requiring that cyber scenarios be undertaken and the results reported.

EY client-serving teams are working at board-level with many leading companies who are undertaking cybersecurity simulations and war gaming to encourage the C-suite to think more broadly and seriously about future threats and opportunities, and helping them to move in the right direction to "Anticipate."

Take action – and get ahead

If your organization is ready to move into the Anticipate level, here are five vital actions we suggest you should take:

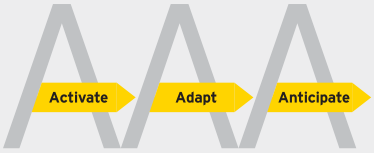
1. Design and implement a cyber threat intelligence strategy
The Information Security function should work with the Board to help them understand how to use threat intelligence to support strategic business decisions and leverage the value of cybersecurity.

2. Define and encompass the organization's extended cybersecurity ecosystem
Work with others in the organization's extended ecosystem to define RACI and trust models and enact cooperation, sharing capabilities where advantageous.

3. Take a cyber economic approach
Understand which are the organization's most vital cyber assets and their value to the cyber criminals, then re-evaluate plans to invest in security.

4. Use forensic data analytics and cyber threat intelligence
Take advantage of the latest technical tools to analyze where the likely threats are coming from and when, increasing your ability to combat them.

5. Ensure everyone understands what's happening
Strong governance, user controls and regular communications will update employees and keep then acting as the eyes and ears of the entire organization.



One organization, three stories

Below is a familiar story, told in three different ways. While this is a fictitious example, the reactions, impacts and events are based on our actual experiences with clients and the events that unfolded during this time. Companies in the different Activate, Adapt or Anticipate phases will identify, react, respond and recover from these incidents in very different ways. We will evaluate the impacts on them:

1. Financially | 2. Operationally | 3. Personally

Our case study involves three versions (Activate, Adapt, Anticipate) of a large telecoms operator (>US$12b in revenue) with significant retail operations (>400 retail and customer service centers) and direct interaction with their customers, both in person and online. They will suffer a breach of customer data and we will watch their very different experiences reacting to very similar events.

Activate

The scenario: This company suffered a significant breach of customer data. The announcement was first released by an external source publicly and ultimately confirmed by the company. The company very quickly responded, confirming the breach had occurred and informing the public they had identified the problem, it had been resolved and the impact was minimal.

However, a week later the same external source stated that the damage was significantly worse than confirmed by the company, and millions of credit card details had been stolen. The company acknowledged this was true. The source made more discoveries, and this back and forth continued in the media for several weeks until eventually it was discovered that the number of records lost was over 10 times the original number quoted and that there was evidence that the breach was still active and not resolved.

Financial: The story played out in the media over a period of two months, right before their busiest time of the year. They lost many customers, but the ultimate cost was double-digit percentage loss in both share price and revenue. The company has still not seen a return to pre-breach numbers (over a year later). Eventually the total cost of the breach is expected to exceed 5% of annual revenue.

Operational: The company spent many months of effort focused on this problem and rather than fixing it, their efforts were focused on responding and managing the media crisis that occurred. They had to identify and provide credit monitoring services, work with banks and customers to settle their concerns and ultimately attempt to restore customer confidence.

Personal: This led to the termination or resignation of many executives and leaders throughout the organization, including both the CEO and CIO.

Adapt

The scenario: This company suffered a significant breach of customer data. The announcement was first released by an external source publicly and ultimately confirmed by the company, but the company did not comment for almost a week. They provided a very measured response, confirming the breach, identifying that they knew where it had occurred, felt confident they had addressed the problem and were waiting to confirm the extent of the problem until the investigation was complete. Two weeks later they came out publicly and confirmed the total loss, confident they had identified the source of the breach, and had put in place mitigating controls and were working on the permanent resolution. Since then there have been no contradicting reports.

Financial: This incident generated three primary news stories, but was in and out of the media fairly quickly. While the breach was significant, the company did not experience a high churn in customers. They did provide credit monitoring, and introduced special offers to bring customers back to the stores, at some cost. Within three months, they had returned to pre-breach revenue, share price and operations.

Operational: This story had left the media spotlight within a month. The company put more time and effort into fixing this problem than responding to media pressure. They had to work with banks, brands and customers and their efforts focused on accretive services and support for the business.

Personal: Throughout this challenging time the company showed solid leadership in the event of a crisis, and sustained the confidence of customers, shareholders and the board.

Anticipate

The scenario: This company suffered a significant breach of customer data. In the months prior to the attack, the company had worked with peer organizations, law enforcement and their internal threat intelligence teams to collect relevant attacker activity information and identify the risks to the company. They also learned about other breaches in their sector. As a result, they were able to develop additional segregation and protective controls, and create scenarios for attack and response exercises. Ultimately, they were not able to stop the attack taking place, but no payment details or sensitive personal information was lost as it had already been stored separately and protected with different controls. Due to additional monitoring, the breach was discovered internally first. Shortly after the incident, the company released a public statement about what had happened and how it had been addressed.

Financial: While the cost of recovery from the breach was significant, the impact on share price, customer churn and media exposure was minimal to none. The cost was confined to investigative and remediation activity. The company was able to control the media attention with enough confidence that they did not need to offer credit monitoring service, which is the usual response to a customer data breach. This alone will save at least US$350m in potential cost of response and, arguably, it strengthened their customers' and regulatory confidence.

Operational: There was virtually no media coverage beyond the statement released by the company itself; they could therefore focus their efforts on returning to business as usual. The cost of investigation and remediation became an additional operational cost, so the breach investigation did not negatively impact their BAU processes and weaken their defences – a frequent error that creates an aftershock affect, which can cause subsequent breaches.

Personal: No terminations or resignations were tabled, and there is evidence of renewed confidence in the executives.

Summary

Where organizations are now

Cyber risks are growing and are changing rapidly. Every day, cyber criminals are working on new techniques for getting through the security of organizations, including yours. They are doing this so that they can cause damage, access sensitive data and steal intellectual property. Every day, their attacks become more sophisticated and harder to defeat.

Because of this ongoing development, we cannot tell exactly what kind of threats will emerge next year, in five years' time, or in 10 years' time. We can only say that these threats will be even more dangerous than those of today. We can also be certain that as old sources of cyber threat fade, new sources will emerge to take their place.

Despite this uncertainty – in fact, because of it – you need to be clear about the type of cybersecurity you need.

What organizations need to do

To get cybersecurity right, the first step is to get the foundations right. Given how much attention recent cyber attacks have received, no one can claim they do not know the dangers; so there can be few excuses for organizations that are still not putting basic cybersecurity systems and processes in place.

Once the foundation has been mastered, the next stage is to make your cybersecurity more dynamic and better aligned and integrated into key business processes. Without taking this crucial step, organizations remain vulnerable – particularly when they, their environment and the cyber threats they face are all changing.

And then comes the real opportunity: the chance to get ahead of cybercrime. By focusing your cybersecurity on the unknowns – the future and your business's broader ecosystem – you can start building capabilities before they are needed and begin to prepare for threats before they arise.

What it is	Cybersecurity system building blocks	Status
Anticipate is about looking into the unknown. Based on cyber threat intelligence, potential hacks are identified; measures are taken before any damage is done.		**Anticipate** is an emerging level. More and more organizations are using cyber threat intelligence to get ahead of cybercrime. It is an innovative addition to the below.
Adapt is about change. The cybersecurity system is changing when the environment is changing. It is focused on protecting the business of tomorrow.		**Adapt** is not broadly implemented yet. It is not common practice to assess the cybersecurity implications every time an organization makes changes in the business.
Activate sets the stage. It is a complex set of cybersecurity measures focused on protecting the business as it is today.		**Activate** is part of the cybersecurity system of every organization. Not all necessary measures are taken yet; there is still a lot to do.

Where we'd like organizations to be

Organizations must look ahead and look beyond the business – new threats are being created today and you need to get ahead of the game. Although this year's survey does not suggest that they will get there soon, we would like proactive, intelligent cybersecurity to become the norm for every organization.

We don't want the focus to be on business-destroying attacks or public relations disasters: we want the focus to be on enhancing the organization because businesses have mastered the foundation; they are introducing innovative new approaches and they are using powerful new tools making them stronger and safer than ever. We would like businesses to take the initiative and make cybercrime far less profitable and a far less effective use of time and resources than it is today. In other words, take away the power of the hacker and get ahead of cybercrime.

How EY can help

At EY, we have an integrated perspective on all aspects of organizational risk, and cybersecurity is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

Our cybersecurity professionals address the challenge of managing the information and cybersecurity risk to business operations. We draw on in-depth industry-leading technical and IT-related risk management knowledge from our global organization to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients' applications, infrastructure and data.

Cybersecurity is regularly discussed in the board room; we know the business impact and technical details and how to present these to C-level executives, resulting in deeper risk insights and more in-depth executive-level discussions. We aim to be a trusted advisor to our clients as they face the challenge of protecting and securing their assets; for example, we help our clients with:

- Aligning their information security strategy with business needs
- Containing and investigating complex cyber breaches, and remediating detect and respond approaches
- Optimizing their information security spending and making their Cyber Program Management (CPM) more cost-effective and sustainable
- Improving SOC capabilities
- Helping monitor, maintain and enforce compliance with access management policies, as well as addressing legal and regulatory compliance related issues
- Assessing adequacy of resources and skills for implementing technology and processes

Our cybersecurity services include key aspects of the **Activate**, **Adapt** and **Anticipate** phases mentioned in this report to help you get ahead of cybercrime.

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

Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem

Cyber Program Management: identifying ways to get ahead of cybercrime

www.ey.com/CPM

Security Operations Centers – helping you get ahead of cybercrime

www.ey.com/SOC

Privacy trends 2014: privacy protection in the age of technology

www.ey.com/privacy2014

Maximizing the value of a data protection program

www.ey.com/dataprotect

Building trust in the cloud

www.ey.com/cloudtrust

Identity and access management: beyond compliance

www.ey.com/IAM

Big data: changing the way businesses operate

www.ey.com/bigdatachange

Survey methodology

EY's Global Information Security Survey was conducted between June 2014 and August 2014. More than 1,800 respondents across all major industries and in 60 countries participated.

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 conducted 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.

Respondents by area (1,825 respondents)

Key:

EMEIA	39%
Americas	26%
Asia-Pacific	22%
Japan	13%

Respondents by total annual company revenue

Key:

US$10–US$50 billion	167
US$1–US$10 billion	441
US$100 million–US$1 billion	479
US$10–US$100 million	314
Less than US$10 million	209
Government, nonprofit	119
Not applicable	215

Respondents by industry sector

Aerospace and defense	63
Asset management	60
Automotive	62
Banking and capital markets	308
Cleantech	2
Consumer products	132
Diversified industrial products and chemicals	146
Government and public sector	119
Health care and Provider care	70
Insurance	138
Life sciences	40
Media and entertainment	44
Mining and metals	43
Oil and gas	55
Power and utilities	68
Private equity	1
Professional firms and services	68
Real estate	56
Retail and wholesale	100
Technology	117
Telecommunications	62
Transportation	71

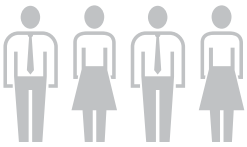
Respondents by number of employees

Less than 1,000	664
1,000 to 5,000	557
5,000 to 15,000	283
15,000 to 50,000	194
50,000 plus	127

Respondents by roles/titles

Chief Information Officer	208
Chief Information Security Officer	283
Chief Security Officer	54
Chief Technology Officer	41
Information Security Executive	233
Information Technology Executive	346
Internal Audit Director/manager	72
Network/System Administrator	38
Other C-suite, Executive, Vice President	60
Other	490

Profile of participants



1,825
respondents

60
countries worldwide

25
industry sectors

Contact us

We have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls, and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance, as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our clients' applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

Our Risk 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		
Ken Allan	+44 20 795 15769	kallan@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

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

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or, more specifically, on achieving growth or optimizing or protecting your business, having the right advisors on your side can make all the difference. Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

EYG no. AU2698

1408-1308388 EC
ED None.

ey.com/giss