

Insights on  
governance, risk  
and compliance

November 2014

# Cyber threat intelligence – how to get ahead of cybercrime



**EY**

Building a better  
working world



## Contents

Introduction . . . . .	1
Why is the cyber threat landscape changing? . . . . .	2
What is cyber threat intelligence? . . . . .	4
How CTI reduces risk . . . . .	6
How CTI provides value . . . . .	8
Conclusion . . . . .	11

# The changing threat landscape

## Cyber threats are increasing ...

In today's cybersecurity landscape, it is not possible to prevent all attacks or breaches; today's attackers have significant funding, are patient and sophisticated, and target vulnerabilities in people and process as well as technology.

With organizations increasingly relying on digitized information and sharing vast amounts of data across the globe, they have become easier targets for many different forms of attack. As a result, every company's day-to-day operations, data and intellectual property are seriously at risk. In a corporate context, a cyber attack can not only damage your brand and reputation, it can also result in loss of competitive advantage, create legal/regulatory noncompliance and cause steep financial damage.

## ... but businesses still aren't doing enough to combat them

Sixty-seven percent of respondents to our *Global Information Security Survey (GISS) 2014\** see threats rising in their information security risk environment. This is why, among our leading clients, cybersecurity is now the number one or number two item on their corporate agenda. It is time to reassess how your organization could be compromised and the impact this could have on its survival.

## Organizations need to take a more proactive approach to cybersecurity

In the evolving threat environment of rapid day-zero attacks, cyber-criminality and espionage activities, the traditional approaches will be increasingly important to maintain, but will simply not be sufficient to properly address risk in individual organizations. Today's secure environment will have vulnerabilities in it tomorrow, so an organization cannot allow itself to become complacent.

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

This report explains why it is important to understand and prioritize cyber threat intelligence processes, and how they can be integrated into an organization's security operations in a way that adds value.



# 37%

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



\*All survey statistics in this report refer to EY's 17th *Global Information Security Survey 2014*, which captures the responses of 1,825 C-suite leaders and information security and IT executives/managers, representing most of the world's largest and most-recognized global companies. Responses were received from 60 countries and across nearly all industries. For further information, please access: [www.ey.com/GISS2014](http://www.ey.com/GISS2014).



# Why is the cyber threat landscape changing?

---

Threat actors are constantly inventing new tools and techniques to enable them to get to the information they want and are getting better at identifying gaps and unknown vulnerabilities in an organization's security.

---

The technology landscape is evolving – fast – and those organizations that don't keep up with it will be left behind. Advanced technologies offer new capabilities and benefits, but they also introduce new risks, and different technologies are being introduced every day, often outpacing the ability to properly assess risk. Whether the people who conduct these attacks are inside the organization or external to it, they use the technologies in place to their advantage.

New business models rely heavily on global digitization, making the attack surface much larger, and exposing gaps in security, especially through the use of cloud, Big Data, mobile and social media – for example, cloud-based services and third-party data storage and management open up new channels of risk that previously did not exist.

Additionally, the “Internet of Things” trend continues – we are seeing companies offer IP-enabled sensors in their products, which may introduce vulnerabilities if they have not been adequately tested. Many of the services we all take for granted operate on the backbone of the internet today and will become more and more connected as time passes. Any direct connection to the internet can mean a direct link to attackers.

But cybersecurity goes far beyond being an IT issue: business activities, such as new product launches, mergers and acquisitions and market expansion, now have a cyber-dimension. We all live and operate in an ecosystem of digitally connected entities, people and data, increasing the likelihood of exposure to cyber adversaries in both our work and home environments.

All of these changes mean that organizations must move to borderless security – but how can they do that safely and securely? There are many obstacles. Our GISS 2014 survey found that there is a significant shortage of people who have the ability and experience to fight back against the persistent hacker and trained in gathering and analyzing cyber intelligence. Budgets are being compressed in every area, and there is often diminishing support from the board to spend more on something that can seem intangible, never mind invest even more on an entirely new proactive approach.

## Threat motivation is changing

Cybercrime is big business and cyber attackers and threat actors take their activities very seriously, but often have differing motivations; for example, **hacktivists** often seek to damage the reputation of an organization as quickly as possible. **Cyber criminals**, on the other hand, seek to gain profit and often run their operations similarly to a legitimate business, albeit with much less ethical consideration. They can convert stolen data into cash or cash equivalent benefits, leading to lost sales, strategic partner hijacking, counterfeit products, patent infringement, negotiation advantage and so forth. A typical breach could impact an organization's public reputation and stakeholder confidence, its market share, revenue and profit, and reduce return on capital and R&D investments.

**State-sponsored espionage** threat actors are likely to be very well organized and industrialized, with vast resources at their disposal; they seek to improve the strategic capabilities of their host nation sponsors by providing them with information about



products, current views, plans, and other data, which can lead to long-term strategic losses (that may not be realized until it is far too late).

Organizations are also being attacked because an attacker wants to exert political influence; for example, an organization that does normal business with another that attackers might consider to be hostile, can itself become a target just because it has a “relationship” there. There is no respect for national boundaries – the attacker can come from anywhere – and it does not matter which country the victim resides in.

And in a new, intriguing twist to the activities of these criminals, some organizations are being held for ransom over the possibility that they have been hacked – leaving them to wonder if it is real or are the so-called “attackers” perpetrating a scam and simply trading on corporate fear? Fake or real, organizations are paying up, which only makes the situation worse for others. This is proof that cyber criminals are less predictable, more persistent, more resourceful, better funded and much more organized.

### How can organizations get ahead of cybercrime?

No single company can possibly match the resources (physical and financial) and the technical know-how of the perpetrators. The reality is that once organizations get on top of one kind of attack, the cyber criminal responds by changing tactics to get in via a different approach. Threat actors are constantly inventing new tools and techniques to enable them to get to the information they want and are getting better at identifying gaps and unknown vulnerabilities in an organization’s security. Discouragingly, attackers often fund their new tools and vulnerability research with money taken from the very organizations victimized before.

To combat these threats, EY has seen an increasing demand for broader solutions to holistically address cybersecurity needs, requiring a combination of identity management and governance, risk and compliance (GRC) solutions.

It’s difficult to know exactly when or where an incident will take place – but by implementing the latest threat intelligence developments, an organization can anticipate and deflect what might happen. Timely identification and reporting of breaches will reduce costs, as well as the incentive of attackers; having a proactive cybersecurity approach will make you a more attractive business partner, and engender confidence in your stakeholders and customers.

“Getting ahead of cybercrime,” the theme for EY’s GISS 2014, is all about knowing what is happening, how it is happening, identifying who is the threat, and determining if and when an attack can happen to you. It is about intelligence gathering, and then having the analytical ability to use that intelligence to make critical and strategic business decisions; however, most organizations currently lack the formal ability to do this.



36%

of respondents to our GISS 2014 do not have a 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.

# What is cyber threat intelligence?

## EY's 17th Global Information Security Survey results are concerning.

74%

of respondents say that their "partially" meets their needs.

42%

do not have a Security Operations Center.

25%

do not have a vulnerability identification capability.

16%

do not have a breach-detection program.

13%

do not have a computer-incident response capability.

8%

do not have a data protection program; a further 26% said that their data protection policies are "informal" or "ad hoc."

Cyber threat intelligence (CTI) is an advanced process that enables the organization to gather valuable insights based on the analysis of contextual and situational risks and can be tailored to the organization's specific threat landscape, its industry and markets. This intelligence can make a significant difference to the organization's ability to anticipate breaches before they occur, and its ability to respond quickly, decisively and effectively to confirmed breaches – proactively maneuvering defense mechanisms into place, prior to and during the attack.

When the nature of the threat is suspected and attributed to a specific threat actor, processes can be adjusted (e.g., deciding what should be done with a piece of targeted malware), countermeasures developed (e.g., if actor X is attacking, it has historically gone after a certain type of information), or develop metrics to trend the attempts over time in order to best posture the organization against losses.

CTI is currently one of the most requested additions to a security posture portfolio for many of EY's clients; however, many struggle to articulate their needs and properly integrate CTI into their existing solutions. It is therefore important not only to be able to prioritize CTI processes, but to understand how they can be integrated into the security operations functions in a way that adds value.

Threat intelligence covers the technical information that provides specific indicators that can be used to locate and mitigate current and potential future threat-actor activity in the environment; this information also provides situational awareness of the threat landscape and helps organizations understand who might be interested in attacking their environment. But for this gathering of information to be truly beneficial, it is necessary to develop a CTI program designed to provide actionable, timely, accurate, and relevant reporting, using both tactical and strategic intelligence.

CTI will not predict the future, nor is it a panacea for cyber security programs. CTI is all about likelihood – utilizing incident history, understanding the internal environment and pinpointing probable targets for threat actors – and keeping an eye toward what is going on out in the world to enable the organization to develop a strong game plan for its defense.

While the need for technical indicators plays a critical role, technical information alone is not enough to completely grasp the context of why certain threats should be prioritized differently from others. The real value is in telling the story of what is likely to happen based on various factors, empowering decision-makers to take proactive measures to reduce risk and enhance governance, and to be able to implement cyber defense capabilities in ways that enhance value and help align security with business.

Layering CTI into security operations at all levels ensures that inputs are provided that improve the organization with the ability to prevent attacks, detect attacks when they do occur, and respond more rapidly to attacks with better countermeasures. This layered integration helps to ensure that critical assets and information remain under the control of the organization and reduces the chances that data is exfiltrated or processes are interrupted.



## Proactive prevention

CTI enables a degree of predictive analysis capability to complicate attacks by understanding the threats against you and the likely targets they pursue.

*Who is likely to attack?*

*What types of assets are they looking for?*

## Monitoring and detection

Information gleaned from CTI and information sharing allows organizations to perform log analysis to identify when attackers are present.

*Is the alert I'm seeing related to something I know to be bad?*

*Can I quickly assign criticality to this and escalate actions?*

## Incident response

If and when an incident occurs, CTI can provide insight for incident-responder activities and mitigation approaches to ensure critical information and assets stay protected.

*What lessons learned from incidents can help to improve proactive protection?*

## The current CTI market

There is no doubt that threat intelligence is a hot item right now. There are many established, excellent threat intelligence companies in the market providing data feeds, analysis, and context and provides for any budget. Some of them roll their threat intelligence into comprehensive technical solutions, like the various incident-response companies; some focus on providing information-sharing environments and threat-information feeds. There are also free lists and crowd-sourced feeds that organizations can access; however, these may or may not be vetted and could contain errors. Additionally, there are a number of feeds that provide data regarding malicious domains, botnet activity, malware data and other high-volume black-list indicators.

Not all threat intelligence providers do the same things. Many provide low-volume, high-confidence indicators and reports; others provide considerable volume with variable confidence, and some providers may focus on one type of threat (e.g., advanced persistent threat or hacktivism). Those who have experience with cyber espionage may tend to provide better APT indicators, while those who focus on the areas of social media may provide better insights into hacktivism activities.

Understanding an organizations' unique threat landscape and the threat actors most likely to cause greater impacts is important for properly matching an integration strategy with the right sources of intelligence. The following graphic represents some of the largest offerings from the CTI vendor space although they are not the only categories; each one of these does, however, require specific means of collecting and analyzing data in order to provide actionable intelligence.

### State-sponsored espionage

- ▶ State-sponsored espionage, also referred to as Advanced Persistent Threat (APT), is typically very quiet and practices operational security.
- ▶ Perpetrators target intellectual property and corporate communications, and look for means to maintain persistent access.
- ▶ The best way for providers to determine APT activity is through internal anomaly detection, in-depth analysis of previous incidents and information-sharing networks.

### Organized cybercrime

- ▶ Organized cybercrime activity is primarily driven by financial gain, but will also target data assets that can be traded to others.
- ▶ Cyber criminals have duplicated several tactics of APT actors, due to their effectiveness, and will target anything of value.
- ▶ Several providers have in-depth collection capabilities regarding organized cybercrime forums and can provide detailed intelligence about cybercrime activities and potential compromises.

### Hacktivism

- ▶ Hacktivism actors can be quite loud in comparison to other threat actors, often using social media to discuss operations and to recruit members to attack a target.
- ▶ They are focused on damaging reputations, causing disruptions and making derogatory statements about organizations they do not agree with.
- ▶ Social media outlets provide considerable intelligence regarding hacktivist intentions, their ongoing operations and their potential targets.

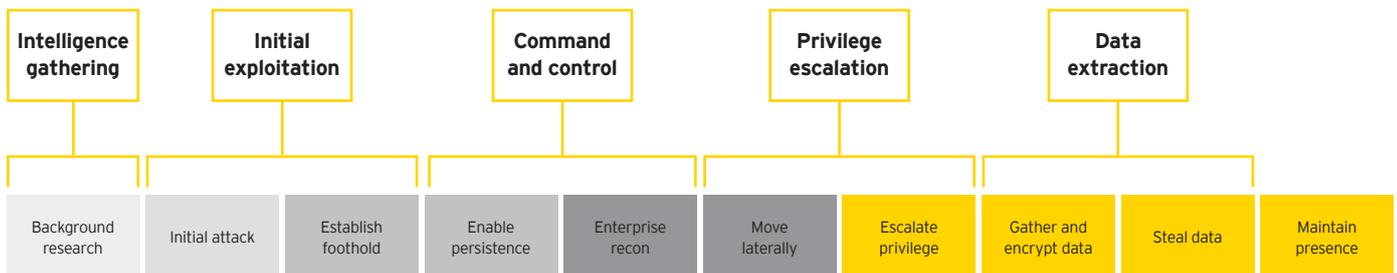


# How CTI reduces risk

The loss of vital or sensitive data, intellectual property or strategic corporate communications to threat actors who pass on this information to global competitors can severely damage the long-term viability of a company. Understanding the likely threats and identifying vulnerabilities earlier will help organizations prioritize preventative and response activities in order to reduce the chances that the attackers will be successful in their goals.

By integrating CTI into various aspects of security operations, it can be used to map out the threat landscape and put historical data into context. As a CTI program matures, predictive capabilities are uncovered, allowing management to make decisions that are based on historical precedent rather than intuition. It can also be applied through metrics analysis to threat-modeling capabilities, allowing organizations to sub-categorize a threat actor's activities, enabling countermeasure employment at a more granular level.

*The following graphic represents EY's point of view on a hypothetical adversary life cycle.*



Utilizing a life-cycle model, the outcome of the analysis will allow the organization's security team to identify which phase of activity they are looking at when things do occur, based on precedent. This is not something that can be accomplished immediately, but if considered early, it will be beneficial for the evolution of the CTI program. By analyzing metrics over a number of intrusion attempts, an organization may also have a timing factor that can be used to employ countermeasures with more agility; for example, if initial attempts at gaining access are identified, it is potentially possible to link that activity to a group who historically gathers all the data to a central location for exfiltration, and positive moves can be made to block it.

Occasionally, what the organization chooses *not* to do based on the threat-actor determination may also be important. Faced with malware that has been specifically designed to target a specific organization, the implications of notifying anti-virus vendors about that variant should be considered; any change will undoubtedly be noticed by the attackers, and they will simply alter their code so that it cannot be picked up; so when they attack again, there will be no way to tell they are attacking. This is a risk decision, which can be made with more confidence if the organization understands the adversary it is facing.



## The challenges for CTI

Those who are using threat intelligence feeds for information gathering often complain about the overload of data that pours in. It can be difficult to handle the volume, so some vendors are trying to focus on quality over quantity. The positive side of that approach is that it is easier to consume a limited amount of data, and it is likely to be very rich, with considerable context. The downside is that there will possibly be certain indicators that will be missed; however, if an organization isn't capable of handling a massive volume of data, the threat indicator may be missed anyway.

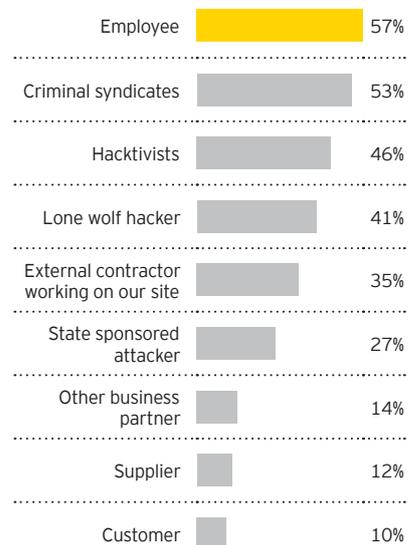
The key for organizations seeking to implement a threat intelligence feed is to ensure that the feed addresses the types of threats that are likely to be active in their environment (see chart at right). Some vendors focus on specific areas and others are broader in their approach: each of these may come with different prices, making the decision to purchase threat intelligence difficult. If unsure, a company could first test the high-volume approach and see what kinds of indicators are prevalent in the environment; once they have a good idea of the kinds of threats attacking and the impact of those can be considered, then the organization can align with a good provider focused on their specific threats, within the right price range.

Another concern for organizations is their relative maturity: this is especially concerning for information-sharing groups. The sharing of information in a larger group, whether ad-hoc, semi-formal, or in a moderated formal environment, is the secret ingredient for organizations who have the most success at understanding, scoping and mitigating intrusions in their networks. It will be critical to try to participate in these forums and ensure that information is flowing from all participants as much as possible in order for the group to retain its value – if a participant starts to become the dominant provider for the group and gets little in return, it will tend to look for new partners to share information with, which may reduce the benefits for all concerned.

Integrating CTI into operations can also be a challenge. Too often, intelligence feeds are purchased and not properly integrated. Analysts may develop a certain degree of situational awareness, but without technically integrating CTI into the existing infrastructure, the organization is missing out on an opportunity to automate processes and increase visibility. This is a waste of an expensive resource. Most, if not all, major intelligence providers have either a managed service component or an API that can be integrated into your SIEM of choice; this helps with the volume problem and reduces the time-lag in applying context to detection.

### Cyber threat actors

Our GISS 2014 asked respondents who or what they considered the most likely source of an attack (they could select all that applied):





## How CTI provides value

---

Companies must mature their operations in sync with their intelligence capabilities in order to maximize their results.

---



58%

of GISS 2014 respondents say that their organization is not focusing on emerging technologies

For CTI to be really useful, it needs to be focused on the priorities of the business, helping to reduce the organization's risk profile by enhancing security operations and business decision-making.

In order for intelligence to accomplish this, several factors have to be considered:

- ▶ Intelligence should strive to be **timely** – it should address an issue that is happening or likely to happen
- ▶ Intelligence should strive to be **accurate** – it should be representative of the actual activity seen
- ▶ Intelligence should strive to be **actionable** – the organization should be able to actually do something with it
- ▶ Intelligence should strive to be **relevant** – the content addressed should be something of value to the business

EY's point of view regarding CTI centers on the concept that companies must mature their operations in sync with their intelligence capabilities in order to maximize their results. A new threat intelligence capability should also result in process changes that allow the organization to be more agile in response to better situational awareness: decisions should be made faster; data should be protected; gaps should be uncovered, prioritized and mitigated.

A company needs to understand the best way to integrate intelligence capabilities. The solutions often already lie within the organization – incident responders, security-monitoring teams, SIEM operators and risk personnel probably have a good idea of where the threats will come from. An often overlooked location that can provide a considerable amount of threat intelligence is the data already sitting inside corporate log repositories and incident-management databases. Additionally, the organization should check out the threat landscape of its industry – it is likely that its risks will be similar, if not the same. The more exposure to different industries that an intelligence analyst, or collection of analysts have, the better they will be at drawing upon that experience for a particular situation.

Companies can approach CTI from both a tactical and strategic perspective. Tactical intelligence, the dissemination of indicators of compromise and perhaps recommendations on incident-response procedures, is very important to an organization's ability to increase its security posture. However, strategic intelligence is also valuable to an organization's ability to make important decisions; it builds upon the knowledge base that tactical intelligence has gathered, along with the metrics generated from integrating with operational cybersecurity. This can provide a considerable number of non-technical process changes and considerations that can greatly reduce risk.



### Example 1: mergers and acquisitions

Mergers and acquisitions (M&A) are clear, time-bound events that can benefit from threat intelligence and good countermeasures. By including cyber threat intelligence into M&A processes, organizations reduce the risks involved by thinking through the potential issues early and preparing for them.

Questions to be considered are:

- ▶ What should you know about the company you are merging with or acquiring?
- ▶ What is its security posture compared to yours?
- ▶ How do you keep discussions secret so that your adversaries do not take advantage of a potential alternate entry point to your network?
- ▶ How can you stop an adversary from stealing all of your intellectual property before you secure it?

### Example 2: periodic events

Focusing efforts around detecting a particular type of activity will create historical precedents and indicators that can be used in the future. Knowing there is a trend is only possible if someone notices or if you are collecting the data around a specific recurring activity; for example, if every year executives attend a specific conference, or hold a quarterly board meeting, this could be a particular target for cyber criminals or espionage activities.

Questions to be considered are:

- ▶ Who else knows about this event?
- ▶ What could a threat actor do ahead of time to access your data?
- ▶ Could anyone send phishing emails directly to the attendees prior to their arrival in the hopes of catching them off guard?
- ▶ Will the event organizer ensure their access methods are intact before the meeting?

---

Intelligence should strive to be timely, accurate, actionable and relevant.

---



63%

of organizations would take longer than an hour to detect an attack



# The future for CTI

As the industry continues to evolve its threat intelligence capabilities, organizations will undoubtedly learn more about what the best practices in this space are. Some organizations have been doing this for a while, but as an industry, it's a fairly new area of focus that is still evolving.

Organizations should be enabled to utilize next-generation security concepts such as: active defense; defending campaigning; and the implementation of countermeasures. The aim should be to move from a reactive state to a more proactive approach – to be able to get ahead of cybercrime. This requires maturity in both baseline controls and threat intelligence; it also requires organizations to have a strong understanding of their environment, especially to understand where their critical information and critical assets are located.

A solid threat intelligence program can also be further unlocked with a good metrics program and analytics as the program matures. Business analytics principles can be applied to the data collected in order to uncover trends, visualize threat activity and enhance overall situational awareness. The ability to understand the trends as they relate to the organization enables better governance, in turn reducing time frames associated with traditional security monitoring and incident-response functions.

Threats change over time, as do risks. A dynamic threat intelligence capability helps to ensure that security operations can also keep up with those changes.

Developing a CTI program brings insight to the specific threats that increase risk in the organization. It leads to better processes and allows an organization to strategically prioritize its defense measures to focus efforts on what can cause the most damage to business. It helps to ensure business continuity and, ultimately, the success of the organization.

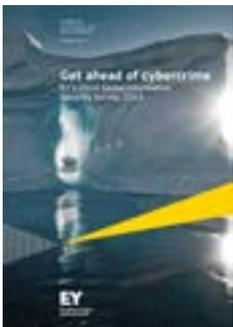
---

Threats change over time, as do risks. A dynamic threat intelligence capability helps to ensure that security operations can also keep up with those changes.

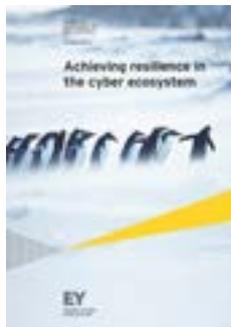
---

# 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](http://www.ey.com/GRCinsights).



*Get ahead of cybercrime: EY's 2014 Global Information Security Survey 2014*  
[www.ey.com/GISS](http://www.ey.com/GISS)



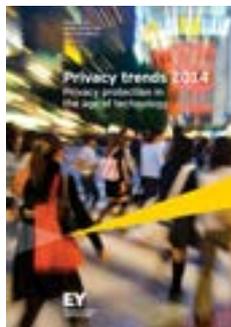
*Achieving resilience in the cyber ecosystem*  
[www.ey.com/cyberecosystem](http://www.ey.com/cyberecosystem)



*Cyber Program Management: identifying ways to get ahead of cybercrime*  
[www.ey.com/CPM](http://www.ey.com/CPM)



*Security Operations Centers – helping you get ahead of cybercrime*  
[www.ey.com/SOC](http://www.ey.com/SOC)



*Privacy trends 2014: privacy protection in the age of technology*  
[www.ey.com/privacy2014](http://www.ey.com/privacy2014)



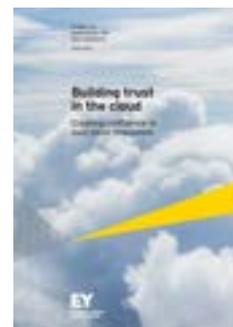
*Maximizing the value of a data protection program*  
[www.ey.com/dataprotect](http://www.ey.com/dataprotect)



*Identity and access management: beyond compliance*  
[www.ey.com/IAM](http://www.ey.com/IAM)



*Big data: changing the way businesses operate*  
[www.ey.com/bigdatachange](http://www.ey.com/bigdatachange)



*Building trust in the cloud*  
[www.ey.com/cloudtrust](http://www.ey.com/cloudtrust)



At EY, 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.

## 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](http://ey.com).

© 2014 EYGM Limited.  
All Rights Reserved.

EYG no. AU2742

1408-1308388 EC  
ED None.



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

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

[ey.com/GRCinsights](http://ey.com/GRCinsights)

## 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.

To find out more about how our Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: [ey.com/advisory](http://ey.com/advisory)

Our Risk Advisory leaders are:

### Global Risk Leader

**Paul van Kessel** +31 88 40 71271 [paul.van.kessel@nl.ey.com](mailto:paul.van.kessel@nl.ey.com)

### Area Risk Leaders

#### Americas

**Amy Brachio** +1 612 371 8537 [amy.brachio@ey.com](mailto:amy.brachio@ey.com)

#### EMEIA

**Jonathan Blackmore** +971 4 312 9921 [jonathan.blackmore@ae.ey.com](mailto:jonathan.blackmore@ae.ey.com)

#### Asia-Pacific

**Iain Burnet** +61 8 9429 2486 [iain.burnet@au.ey.com](mailto:iain.burnet@au.ey.com)

#### Japan

**Yoshihiro Azuma** +81 3 3503 1100 [azuma-yshhr@shinnihon.or.jp](mailto:azuma-yshhr@shinnihon.or.jp)

Our Cybersecurity leaders are:

### Global Cybersecurity Leader

**Ken Allan** +44 20 795 15769 [kallan@uk.ey.com](mailto:kallan@uk.ey.com)

### Area Cybersecurity Leaders

#### Americas

**Bob Sydow** +1 513 612 1591 [bob.sydow@ey.com](mailto:bob.sydow@ey.com)

#### EMEIA

**Ken Allan** +44 20 795 15769 [kallan@uk.ey.com](mailto:kallan@uk.ey.com)

#### Asia-Pacific

**Paul O'Rourke** +65 6309 8890 [paul.orourke@sg.ey.com](mailto:paul.orourke@sg.ey.com)

#### Japan

**Shinichiro Nagao** +81 3 3503 1100 [nagao-shnchr@shinnihon.or.jp](mailto:nagao-shnchr@shinnihon.or.jp)