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

A close look at cyber threat intelligence
Contents

Introduction 1
What does “cyber threat intelligence” mean? 3
What can CTI do for you?
How industry is leveraging CTI 6
The case for operationalizing CTI 10
The future of cyber threat intelligence 14
Introduction

Cyber threat intelligence: bringing clarity or adding confusion?

The market offers many different descriptions of cyber threat intelligence (CTI), and mostly these comprise of different types of information feeds that are not necessarily aligned to any particular organization or industry. At its heart, any sort of threat intelligence is simply assessed information, and can only be understood in the context within which it is created and the proposed purpose of its use. The purpose is usually to increase awareness of defined situations and environments and to aid in decision-making, at either an operational, tactical or strategic level.

Therefore, it is necessary for organizations to understand how threat intelligence can increase your understanding of relevant situations, and which decisions it can contribute to.

Without this thinking and framing of purpose, organizations will not know which questions to ask of all the available information (whether internally or externally sourced) to refine the collection of information and help direct the analysis. Nor how to incorporate the intelligence in decision-making processes. For cybersecurity, much of this thinking and prioritization is incorporated into systems that are programmed to collect and monitor information, but the human analysis component remains crucial.

In general, organizations do not yet fully understand what to ask of CTI, or how to understand the different “levels.” For more operational roles, e.g., those associated with a security operations center (SOC), CTI will be very technical and closely related to vulnerability information; while to the CEO, “cyber threat intelligence” may equate exclusively to headlines or reports they receive on various cyber events, which may not help them understand how they could be relevant to their organization.

From EY’s point of view, this lack of understanding and/or the limited application currently associated with CTI means that many organizations are missing out on one of the most powerful opportunities of the digital age – the chance to get ahead of the cyber criminal.

A robust CTI program can shed light on a multitude of strategic business concerns and risks, while providing highly technical actions, countermeasures, and metrics to the cybersecurity program at large. It can potentially provide answers to questions like:

- What are the most significant threats facing our organization?
- What assets are (potentially) being targeted, and by whom?
- How can our organization protect against these cyber threats?
- How can our organization use intelligence to augment and improve our security and business operations?

By building a CTI program, organizations are able to simultaneously mature existing cybersecurity processes and develop overarching insight into their specific threat landscape.

36% of GISS 2016 respondents say it is unlikely they would be able to detect a sophisticated attack

Results shown in this report are based on findings from EY’s Global Information Security Survey 2015 – ey.com/giss2015
What does “cyber threat intelligence” mean?

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.

The process manages the collection, analysis, integration and production of previously disjointed information for the purpose of extracting holistic, evidence-based insights regarding an organization’s unique threat landscape. 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.

CTI focuses on identifying and analyzing the motivations, methods, capabilities and tools of adversaries who may seek to target an organization by pairing external analysis with data that was once segmented within the enterprise. While some organizations may choose to define CTI as solely a component or input driven service, it is important to note that a process based intelligence life cycle within an operational framework is required to deliver actionable results.

Accordingly, a holistic CTI program consisting of processes for collecting, producing and disseminating tactical and strategic intelligence, continually augmented with timely situational awareness updates (also known as “current intelligence”), is required. This helps explain who the relevant adversary is, how and why they may be attacking the organization, what actions they could take following the initial compromise, where they may reside within the organization, and how to detect or respond to an attack.

How do you find the criminals before they commit the cybercrime? – A close look at cyber threat intelligence
What does “cyber threat intelligence” mean?

What can CTI do for you?

Organizations may already be investing in various intelligence feeds and reports, but many are still finding themselves asking: “what can cyber threat intelligence do for me?” The breadth and diversity of EY’s answer is often surprising:

- **Cyber threat intelligence is more than data and technology – it is analyst expertise, refined methodologies, and process-driven integration**

  The breadth and diversity of CTI value is not realized when investment is exclusively in data and technology such as threat intelligence feeds or intelligence platforms. CTI must be integrated into security and business processes, tailored to the organization’s unique challenges, and supported by trained analysts who use rigorous methodology.

- **Cyber threat intelligence paints the bigger picture for key decision-makers and places security operators ahead of the cyber attacker**

  As the technology ecosystem continues to deliver a stream of disruptive innovations that have positive implications for both organizations and individuals, the cyber criminal is relentlessly discovering new techniques for attacking anything, ranging from medical devices to motor vehicles that can be connected to the internet (see www.ey.com/IoT). Faced with this expanding global attack surface, organizations can be overwhelmed by the amount of noise related to cyber attacks and the potential impacts those attacks may have for their business.

  Even when an organization possesses security data that could be used to inform decision makers, information is often spread across the business in such a way that establishing a single, business-centric view of the organization’s unique threat landscape appears out of reach.

  With cybersecurity at the top of the agenda in many boardrooms, EY believes that organizations require access to bespoke strategic insights that will inform leaders of the most salient threats facing their organization. CTI delivers these insights by integrating previously siloed security data from across the enterprise with external context to provide a holistic perspective of the organization’s threat landscape. This integrated approach strengthens the organization’s security posture by empowering stakeholders with an informed perspective on how cyber threats are relevant to their areas of responsibility. Additionally, CTI can empower a proactive approach by introducing a robust operational framework to counter adversaries that includes the proper governance structure and security operations maturity.

- **Cyber threat intelligence is the enabler to more proactive security approaches**

  Simply reacting to a cyber adversary’s actions against your organization is certainly not an ideal security posture. EY’s believes that taking an Active Defense approach will enhance the organization’s current cybersecurity and focus operations on preventing the enterprise’s most likely adversaries from achieving their specific objectives (theft, fraud, market manipulation, etc.) This focus is realized from insight generated by an integrated Cybersecurity Transformation program combined with analytical CTI.

78% of GISS respondents do not use a standardized cyber threat intelligence sharing solution
Active Defense

The “active” part of Active Defense is realized by the execution of deliberately planned sets of defensive operations that are known as “missions.” The use of the term “mission” conveys the fact that the operational process proceeds with a significant amount of analytical rigor and discipline in order to achieve maximum effectiveness in accomplishing the organization’s security goals. Missions are planned in response to specific threat intelligence in the unique context of the defended organization.

**Active Defense benefits are clear:**

- For the security operations team, Active Defense provides a defined set of improvement activities rationalized by CTI and connected to achievable objectives. The team builds countermeasures, hunts hidden intruders, and fortifies defenses based on real reporting about the behavior of real attackers.

- For decision-makers, Active Defense connects resource deployment directly to measures of cybersecurity program effectiveness. Instead of focusing on performance measures like the “number of patches applied” and the “number of tickets closed,” effectiveness is demonstrated via a decrease in successful targeted attacks and a decrease in the time required in discovering and eradicating the attacks that were successful.

*For more information, please see [www.ey.com/activedefense](http://www.ey.com/activedefense)*
How industry is leveraging CTI

By attaining evidence-based insight to cybersecurity and the threat landscape, CTI can be delivered and leveraged in many ways to inform decision-makers at all levels from security analyst to the most senior executives.

Today’s market emphasis is on delivering CTI in the form of subscriptions and intelligence visualization platforms; but because subscriptions and intelligence visualization platforms are not supported by an operational framework, they result in a reactive security posture rather than an Active Defense mindset.

A robust operational framework ensures that security operations are mature enough to ingest relevant intelligence and enables timely actions. Such a framework would need to include more than technological maturity, but also processes and governance that are addressed when an organization invests in developing an indigenous intelligence capability, rather than only purchasing external intelligence mechanisms. However, in many organizations these core framework considerations are often passed over, or insufficiently developed, to keep up with a dynamic, ever-changing threat landscape.

One of the primary constraints organizations face when considering a mature CTI capability is cost. Developing a robust intelligence capability can be expensive, which means that finding the right balance of purchased services and incremental growth is pivotal. Additionally, purchased services such as subscriptions and intelligence platforms come with their own set of challenges: for example, these types of services are often tailored toward a technical audience and lack industry focus – this poses a challenge for executives who require business risk-centric analysis on industry-specific threats that can be leveraged for strategic planning.

EY’s GISS 2015 asked 1,755 respondents “Which statement best describes the maturity of your threat intelligence program?” (Select one)

- We do not have a threat intelligence program: 36%
- We have an informal threat intelligence program that incorporates information from trusted third parties and email distribution lists: 30%
- We have a formal threat intelligence program that includes subscription threat feeds from external providers and internal sources, such as a security incident and event management tool: 20%
- We have a threat intelligence team that collects internal and external threat and vulnerability feeds to analyze for credibility and relevance in our environment: 10%
- We have an advanced threat intelligence function with internal and external feeds, dedicated intelligence analysts and external advisors that evaluate information for credibility, relevance and exposure against threat actors: 5%
Subscriptions

Not all threat intelligence subscriptions provide 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 threats, cybercrime or hacktivism). This intelligence may come from dark web or deep web analysis, proprietary collection mechanisms and/or analysis of open source information.

The process of identifying and vetting data that is valuable for a specific organization is challenging due to the sheer volume of these types of open, paid and internal sources. Even when sources are selected and data collection begins, many organizations are not capable of ingesting the full scope of what is provided (e.g., Indicators of Compromise (IOCs)), or determining action from data-heavy reports. Importantly, pivotal context surrounding information provided in feeds and reports is often missing, leaving the organization trying to understand the relevance without the background of why the data is important.

Subscriptions should not just be limited to the automatic integration of feeds and electronic delivery of reports, but rather should be custom-fitted to the industry and the organization’s needs in order to enable actions. This can be achieved by the provider working with the organization to determine the right selection of subscription offerings, which can be a combination of:

- Tailored technical indicator feeds for automatic integration
- Informative webcasts and training events to target the operationalization of threat intelligence
- Analyst-delivered briefings to inform both security operators and executives
- Industry- and business-specific reporting on current events, emerging cyber threats and trends on customized time schedules to meet operational needs (daily, weekly, etc.)
- Timely event-driven updates with analysis on significant and relevant cyber events

Having direct analyst support to deliver products, provide briefings, answer intelligence related questions, and tailor analysis and recommendations to an organization’s threat landscape is pivotal for maximizing the use of subscription services.

Intelligence platforms

Some threat intelligence solutions provide a combination of feeds in a technological platform that enable visualization of data, and with such a large number of cyber threat intelligence providers to choose from, organizations can be tempted to select vendors offering this type of pre-configured, stand-alone solution because these types of vendors are often immediately available and can initially appear to be more cost-effective. However, upon purchasing this service, organizations often realize that they have been left to make that data actionable and relevant for themselves, have little ownership of the data, and are at potential risk for contract fee increases while not fully realizing the value of their purchase.

Intelligence platforms can be a crucial component to cybersecurity when combined with key processes within a mature intelligence program to visualize collected data and support long-term trending. Trending analysis can provide valuable insight specific to the organization and to industry by showing changes in adversary tactics, techniques, and procedures (TTP) over time, and patterns in intelligence of value determined when key stakeholders take the time to document their intelligence requirements. This analysis is most effective when captured in a way that leaders find meaningful to business risk decision-making and the prioritization of countermeasures and remediation activities.
How industry is leveraging CTI

CTI market development

The development of mature CTI programs within a cybersecurity framework is the natural evolution of threat intelligence services beyond purchased subscriptions, feeds, and technical platforms. It is a long-term investment, which requires dedication and key stakeholders that can realize the lasting benefits this type of service provides. These long-term visions among stakeholders are emerging despite conducting business in a world that promotes smaller immediate value to cybersecurity over growing a more mature and secure posture over time. Intelligence services of this kind include a customized approach to governance, people, processes, technology and data.

A robust CTI integration is grounded in tailored assessments that answer specific stakeholder questions, consider the organization’s unique threat landscape, and provide immediate operational value with thorough recommended actions. To support this, organizations should consider developing a CTI program and also conduct a periodic assessment of how the threat landscape might affect them.

> CTI programs

A CTI program will help to enable the capability within an organization’s security operations structure to collect, analyze, produce and integrate its own and external intelligence. The design, build, and operations development of a CTI program supports simultaneous growth within corresponding security operations, allowing the organization to ingest increasingly more robust threat intelligence, subsequently keeping the business from being overwhelmed by data: this also allows them to take actions they are ready for, and to identify what must be additionally matured to take further actions.

> CTI assessments

Currently, in the marketplace there are gaps between an organization digesting threat intelligence and an organization then integrating the intelligence into operations. A common theme is frustration with where to start.

CTI can be implemented incrementally, allowing small investments to improve and mature other areas of cyber threat management in a way that maximizes return on investment.

Tailored assessments gather the pertinent facts and organize the pros and cons of various program attributes to promote a process-oriented approach, providing immediate insights and an evaluated look at where organizations can start integrating CTI. These assessments can answer specific business questions providing a clear way forward through recommendations.
The case for operationalizing CTI

A common challenge that permeates the industry is how best to make use of CTI:

- How can an organization go about making CTI relevant and actionable?
- How can an organization integrate relevant and actionable intelligence into security operations?

Purchasing threat intelligence subscriptions, feeds, and/or reporting does not answer these questions; neither does installing a cutting-edge threat intelligence platform. Only through the unearthing of an organization’s unique CTI requirements and the designing of custom integration processes can the organization truly operationalize CTI.

However, EY has noted several issues that limit the operationalization of CTI. One issue is a lack of consolidation of intelligence sources (i.e., multiple subscriptions owned by the organization used by different divisions and not shared); another issue is the inability to maintain platforms or integrate intelligence results in shelved appliances; other organizations may have an inability to properly integrate purchased intelligence feeds into security technologies, which limits the ability to use the intelligence purchased in a meaningful way.

Intelligence requirements

Intelligence requirements are how an organization steers and scopes their CTI efforts in order to ensure they gain the right insight and the ability to operationalize the intelligence. The requirements are specific and singular questions that an organization does not currently have a complete or current answer to and whose answer will add value to the business. Requirements should be developed based on multiple stakeholders operations, concerns and gaps in knowledge. In this way, the intelligence requirements will take on the shape and feel of the organization and become equally unique and diverse. For example, a manufacturing organization with a global presence will have global supply chain-related intelligence requirements, whereas a regional financial organization may not.

By identifying specific questions that an organization needs answered, they can target their intelligence collection and production to support operations and decision-making.

Intelligence collection should take place both internally and externally to the organization. Internal data collected might include network event data, vulnerability scan data, and incident response reporting. Externally-derived data could include deep and dark web activity, social media and forum discussions, geopolitical news, and third-party reporting on adversaries and their activities.

Many companies choose to purchase their externally derived intelligence through subscriptions and feeds. There are so many options and combinations of external and internal data to collect that deciding what to collect or purchase can be daunting. Many organizations end up with data fatigue and significant amounts of data that they are not making use of, resulting in an absence of operationalizing CTI. By predefining intelligence requirements, an organization can focus its efforts and determine the most relevant cross section of collected sources for the organization.
It is not enough to simply collect the data — it must be used to paint the bigger picture of what is happening in the organization’s threat landscape. To do this, the data must be monitored, analyzed, trended, quantified into metrics and then delivered to the appropriate audience to take action upon — daily, weekly, monthly, quarterly, yearly and even on-demand reporting can all serve to complete this picture.

Intelligence production must answer different groups of stakeholder questions to the right level of operational detail, in a timely manner and in an ingestible format. In this way, purchasing reporting, which is sold to multiple organizations, often does not account for the specific operational needs of your own organization, and it is for this reason that more and more organizations are asking how to make use of threat intelligence reporting. Uniquely defined requirements, focused collection, and operational driven production are the answers.

Using the intelligence to support the entire organization

**Cyber threat intelligence supports both decision-makers and security operations**

Collected and produced CTI must be integrated through processes designed to support both decision makers and security operations. The input processes and output products of a CTI program should be designed with the goal of improving cyber threat awareness across the entire organization at a variety of levels. EY believes that this can be achieved when CTI is viewed through the lens of “tactical,” “strategic” and “current” intelligence components and delivered to relevant stakeholders.

**CTI program components**

<table>
<thead>
<tr>
<th>Tactical intelligence</th>
<th>Strategic intelligence</th>
<th>Current intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>▶ Acts as a force multiplier for internal security operations to improve organizational threat posture</td>
<td>▶ Translates cyber threats into business risk</td>
<td>▶ Rapidly delivers early warnings of the latest threats to stakeholders across the organization</td>
</tr>
<tr>
<td>▶ Provides technical intelligence that can be rapidly integrated within an organization’s native sensor and first line of defense capabilities</td>
<td>▶ Empowers business decision-makers to prioritize short-term strategic actions</td>
<td>▶ Drives agile, flexible strategic and tactical intelligence functions</td>
</tr>
<tr>
<td>▶ Leverages adversary life cycle analysis to refine various security operations functions</td>
<td>▶ Translates cyber threats into business risk</td>
<td>▶ Same-day analysis of emerging vulnerabilities with suggested remediation actions</td>
</tr>
</tbody>
</table>

47% of organizations say their information security function reports to board-level stakeholders less than twice a year.
Strategic-level intelligence analysis processes that directly support business operations include prioritization analysis, risk assessments, and predictive analysis. All of these analytical processes require robust data sets and entail painstaking trending and analysis, but they provide valuable insight that can support decision-makers.

Tactical level intelligence analysis processes directly support SOCs around the adversary life cycle analysis.

By analyzing adversary activity across the life cycle of actions taken by the cyber criminal, tactical CTI analysts are able to:

1. Integrate known adversary tactics, techniques, and procedures into various security operations
   - a. Focus more precise efforts to identify the adversaries’ activities earlier in the life cycle
   - b. Target efforts to locate adversaries and identify damage post-breach

2. Develop threat models that illustrate likely adversary activity
   - a. Informed analysis on adversaries likely to impact the organization, which assets they may target, and what network paths the adversary may take
   - b. Provide threat models to attack and penetration professionals to actively emulate likely attacks

3. Create the first line of defense for internally derived network collection
   - a. Collect essential network event data that supports strategic trending an analysis
   - b. Provide network activity insight beyond the length of log capture
Current intelligence processes support both business operations and security operations by focusing on getting the most timely data and rapid analysis to various analysts and stakeholders. Current intelligence analysts are the first line of defense for identifying relevant external intelligence and routing it to the parties that need to operationalize the intelligence. In this way, current intelligence is pivotal in ensuring timely operationalization of CTI.

All levels of intelligence are operationalized into remediation and countermeasure operations. In fact, intelligence-driven countermeasure operations are a guiding principal to EY’s point of view on **Active Defense** — a deliberately planned and continuously executed campaign to identify and eradicate hidden attackers and defeat likely threat scenarios targeting your most critical assets.

Intelligence-driven remediation and countermeasure operations include processes that enable the operationalization of CTI:

- Threat intelligence support to incident response plans
- Alerting upon and recommending actions for vetted current intelligence
- Targeting security operations along the paths of developed threat models.

All of these processes will be unique to your organization’s operations and challenges.

The case for CTI — example scenario

With the rapidly changing threat landscape and the impact of attacks seemingly becoming higher, getting ahead of potential attacks and vulnerabilities has been a major win for some organizations that have improved their CTI capabilities. For many organizations without insight into what is changing or further, insight into what their own current posture is, getting panicked questions from executives can make an already complicated situation that much more stressful.

During several of the recent breaches where a specific attack vector or vulnerability has been used, the organizations’ security teams not only were able to address those questions, but in some cases pre-empt the discussion with a call to state that they were aware of what was happening, and able to state if they were secure against the specific threat or, if not secure, what the teams were doing to remediate the situation quickly.

These types of wins not only reduce stress for the security team, but also bolster confidence in the abilities of the security team.
Conclusion

The future of cyber threat intelligence

Despite CTI not being fully proliferated within the marketplace, organizations will need to continue to adapt to change in the cyber threat landscape to better understand how threat intelligence can reduce their over-all business risk. CTI discussions surrounding business risk rather than just security risk will become more and more common. Understanding cyber threat risks to the business’s finances, reputation, information and operations will continue to broaden the discussion beyond a security or technology audience.

Short-sighted and pressured organizations will continue to buy threat intelligence feeds and technologies, without aligning such investments to a long-term vision for governance, integrated processes and unique business requirements. However, more and more companies will begin focusing on building a robust threat intelligence capability and/or using tailored intelligence to answer their specific business questions; this will lead to greater investments in the process design surrounding CTI and industry/or organization tailoring of threat intelligence.

Leading organizations will focus more heavily on customizing available CTI on their own, and become more willing to share threat intelligence with others in their ecosystem in order to make the threat intelligence actionable; this will lead to a greater distaste for proprietary protection of valuable intelligence context from intelligence vendors. In turn, CTI vendors will need to become more focused on providing details on how the adversary operates (dynamic indicators) than on sharing singular indicators of compromise (static indicators) that lack context.

The financial and government sectors will continue to lead the way in process-driven integration of CTI and information sharing. Industries with increasing risk and unique challenges, such as oil and gas, retail, health care, food and agriculture will increase investment in the area of CTI and, as these industries continue to evolve their threat intelligence capabilities, and they will undoubtedly contribute to the further development of the best practices in cybersecurity.

CTI will help to enable organizations to leverage next generation security concepts such as: threat modeling, Active Defense, and advanced countermeasure operations. The aim will be to develop repeatable processes that are effective for all organizations in transitioning from a reactive security posture to a proactive approach. Organizations will better appreciate the need for understanding their own environment at a much deeper level in order to achieve this.

There will be increased investment in the detailed mapping of networked environments, the long-term storage and visualization of security operations data, the identification and valuation of high value assets, governance and process design surrounding currently siloed security capabilities, the war-gaming of cyber scenarios against such assets, and the testing of countermeasures.

Threats change over time, as do risks. EY believes that CTI processes can help organizations get ahead of those threats, mitigate the risks, and ultimately, ensure the success of the organization.
EY provides CTI advisory services around assessments, program builds, program support, and subscription services to clients around the globe. EY can also enable seamless integration for organizations wanting to integrate third-party cyber threat intelligence into security operations. Additionally, EY can help bridge the gap between tactical and technical aspects of CTI and help enable more strategic discussions that impact business decision-making.

Throughout the development and maturation of a CTI program, EY:

- Supports clients in maturing their processes to be able to ingest increasingly more robust threat intelligence
- Helps create the in-house capability to translate technical/tactical intelligence into strategic insights for business decision-makers
- Helps prevent clients from drowning in data and produces relevant intelligence
- Provides a personalized look at our client’s threat landscape and identifies what must be matured to take further action
- Pinpoints key internal/external information-sharing opportunities
- Assists with technology selection and solutions architecture

How can EY help?
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 EY’s perspective.

Please visit EY’s *Insights on governance, risk and compliance* series at: [ey.com/GRCinsights](http://ey.com/GRCinsights).

---

Want to learn more?

**Cyber threat intelligence:** Designing, building and operating an effective program  
[ey.com/CTIservices](http://ey.com/CTIservices)

**Creating trust in the digital world:** EY’s Global Information Security Survey 2015  
[ey.com/GISS2015](http://ey.com/GISS2015)

**Enhancing your security operations with Active Defense**  
[ey.com/activedefense](http://ey.com/activedefense)

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

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

**Cybersecurity and the Internet of Things**  
[ey.com/IoT](http://ey.com/IoT)

**Using cyber analytics to help you get on top of cybercrime:** Third-generation Security Operations Centers  
[ey.com/3SOC](http://ey.com/3SOC)

**There’s no reward without risk:** EY’s global governance, risk and compliance survey 2015  

**Unlocking the value of your program investments:** How predictive analytics can help in achieving successful outcomes  
[ey.com/PRM](http://ey.com/PRM)
If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization's defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of back-office systems and into critical infrastructures such as power generation and transportation systems.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then collaborate with you to create innovative answers that help you activate, adapt and anticipate cybercrime. Together, we help you design better outcomes and realize long-lasting results, from strategy to execution.

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

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

© 2016 EYGM Limited. All Rights Reserved.

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.

© 2016 EYGM Limited. All Rights Reserved.

EYG no. AU3750
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

About EY’s Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people advisory, program management and risk – with a complete understanding of a client’s most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory’s high-performance teams also draw on the breadth of EY’s Assurance, Tax and Transaction Advisory service professionals, as well as the organization’s industry centers of excellence, to help clients realize sustainable results.

True to EY’s 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory’s global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

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

Our Risk Advisory Leaders are:

<table>
<thead>
<tr>
<th>Global Risk Leader</th>
<th>Area Risk Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paul van Kessel</td>
<td>Americas</td>
</tr>
<tr>
<td></td>
<td>Amy Brachio</td>
</tr>
<tr>
<td>+31 88 40 71271</td>
<td>+1 612 371 8537</td>
</tr>
<tr>
<td></td>
<td>Jonathan Blackmore</td>
</tr>
<tr>
<td></td>
<td>+971 4 312 9921</td>
</tr>
<tr>
<td></td>
<td>Asia-Pacific</td>
</tr>
<tr>
<td></td>
<td>Iain Burnet</td>
</tr>
<tr>
<td></td>
<td>+61 8 9429 2486</td>
</tr>
<tr>
<td></td>
<td>Japan</td>
</tr>
<tr>
<td></td>
<td>Yoshihiro Azuma</td>
</tr>
<tr>
<td></td>
<td>+81 3 3503 1100</td>
</tr>
</tbody>
</table>

Our Cybersecurity Leaders are:

<table>
<thead>
<tr>
<th>Global Cybersecurity Leader</th>
<th>Area Cybersecurity Leaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ken Allan</td>
<td>Americas</td>
</tr>
<tr>
<td>+44 20 795 15769</td>
<td>Bob Sydow</td>
</tr>
<tr>
<td><a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a></td>
<td>+1 513 612 1591</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:bob.sydow@ey.com">bob.sydow@ey.com</a></td>
</tr>
<tr>
<td></td>
<td>EMEIA</td>
</tr>
<tr>
<td></td>
<td>Scott Gelber</td>
</tr>
<tr>
<td></td>
<td>+44 207 951 6930</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:sgelber@uk.ey.com">sgelber@uk.ey.com</a></td>
</tr>
<tr>
<td></td>
<td>Asia-Pacific</td>
</tr>
<tr>
<td></td>
<td>Paul O’Rourke</td>
</tr>
<tr>
<td></td>
<td>+65 8691 8635</td>
</tr>
<tr>
<td></td>
<td>paul.o’<a href="mailto:rourke@sg.ey.com">rourke@sg.ey.com</a></td>
</tr>
<tr>
<td></td>
<td>Japan</td>
</tr>
<tr>
<td></td>
<td>Shinichiro Nagao</td>
</tr>
<tr>
<td></td>
<td>+81 3 3503 1100</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:nagao-shnchr@shinnihon.or.jp">nagao-shnchr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>