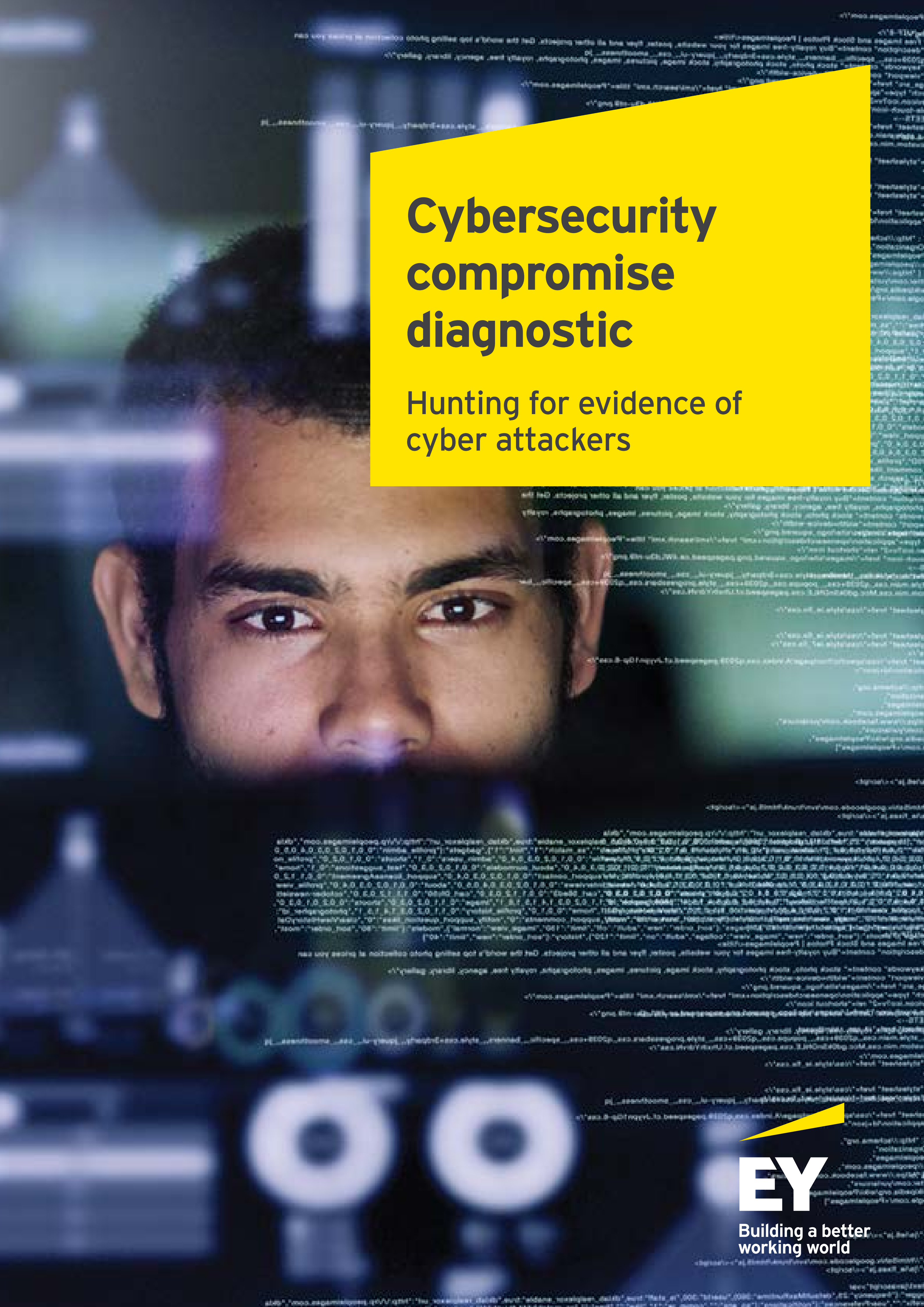


Cybersecurity compromise diagnostic

Hunting for evidence of cyber attackers

Building a better working world

Table of contents

An inescapable imperative

Take the word "prevent" out of the dictionary because organizations recognize that stopping sophisticated cyber attackers is unrealistic.

It's no longer a matter of if or when you will be breached, it has probably already happened.

The quickest way to identify and eject an intruder is to assume that they're already in your environment and to proactively assess your systems and networks for evidence of compromise.

How would you know?

Cyber attacks make headlines on a daily basis. It's no longer a question of if your organization will be breached, or even when, it's likely to have happened already.

Cyber attacks are complex and motivated by a variety of factors, ranging from ideology and financial gain to commercial espionage and even nation state-driven agendas.

The threats are constantly evolving, targeting all organizations, while becoming more prevalent and high-profile. Attackers today are patient, persistent, and sophisticated, and attack not only technology, but increasingly people and processes. Criminals are targeting commercially sensitive information, intellectual property and critical network infrastructure. These threats may come from attackers both within and outside your organization.

Some of these may seem harmless and others far more damaging and malicious in their intent. Nevertheless, any intrusion into an organization's computer systems can lead to operational expense, reputational damage and loss of competitive advantage, not to mention regulatory fines. No organization wishes for its closely guarded secrets to be traded or leaked, or its brand to suffer from adverse media attention.

Many vendors are creating products and services to help counter the threat. Organizations are deploying sophisticated virus detection tools, intrusion detection systems and data leakage prevention appliances. Organizations are also implementing sophisticated vulnerability management programs to identify and remediate vulnerabilities in a timely manner. Despite this array of available technology solutions, attackers continue to find a way through, resulting in high-profile and damaging breaches that continue to be publicized in the media.

As media reports of significant breaches indicate, the challenge lies in detecting evidence of an intruder and taking steps to stop the attack before your data is stolen and real damage is done to your business.

The current cyber threat landscape has a wide variety of threat actors with a multitude of specialized attack capabilities at their disposal. EY's cybersecurity compromise diagnostic services are a set of services which are built to help detect those threat actors via a set of diagnostic assessments.

Statistics sourced from
http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

87%

of board members and C-level executives have said they lack confidence in their organization's level of cybersecurity.

33%

of organizations say it is unlikely that they would be able to detect a sophisticated attack.

44%

do not have an Security Operations Center.

64%

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

Today’s silent intruder

Many attacks, such as Distributed Denial of Service (DDoS), are noisy and disruptive, making them hard to overlook. However, the most impactful attacks tend to be perpetrated by cyber threat actors that are commonly referred to as advanced persistent threats (APT), who use sophisticated and stealthy methods to carry out system breaches that go undetected for extended periods of time.

While every attack is different and is unlikely to follow the same approach (cyber criminals don’t exactly follow a rule book!), it is possible to map the majority of attacks to a simple 10-step process as outlined here. Mapping the attack life cycle in this manner allows an organization to not only understand how an attacker might perpetrate an attack, but also what controls are in place to sense, resist and react to an attacker at each step. It’s these opportunities to terminate an attack early in the process that lead to the mapping process being called the “kill-chain.”

The example here depicts a typical APT attack that starts with spear-phishing. However, the techniques to gain that initial foothold are many and varied, ranging from exploiting vulnerabilities on internet-facing systems through physical breach of defenses and plugging straight into your core systems. We have also included a high-level view of the types of evidence that might exist, and can therefore be detected, at each stage of this example attack.

Attack Life cycle	**Intelligence gathering**	**Initial exploitation**	
	Recon	Initial attack	Establish foothold
What happens	Cyber criminal identifies and focuses on individual attack targets	Email attachment is weaponized with an exploit and delivered through a phishing email	User opens attachment, exploit is installed and calls back to home (C2)
	1	2	3
Typical evidence of compromise	Threat intelligence feeds, dark web forum chatter, early stage attack phishing emails used to test defenses	End-user reports, email server logs, intrusion prevention systems that detect attempted attacks	Malware protection and end-point behavioral analysis, as well as end point logs

Stealth reconnaissance		Privilege escalation		Funds transfer		Clean up
Enable persistence	Enterprise recon	Lateral movement	Escalate privileges	Identify and access targets	Actions on objectives	Remove evidence
Cyber criminal controls user's computer and obtains local privileged access	An internal network hunt is undertaken, mapping out key internal targets	Privileged accounts are identified as they are used and then compromised	Directory store is identified and access to all domain-level accounts is achieved	Sensitive data and/or financial systems are identified and accessed	Data is encrypted and extracted and/or fraudulent transactions are executed	Accounts, log files, etc., are removed to cover evidence of the attack
4	5	6	7	8	9	10
Logs showing use of local privilege accounts and creating of additional local accounts (which can be used by the attacker to get back in later)	Internal network traffic and firewall logs showing systems probing	Access control logs on the hosts identified, as well as installation of hacking tools and/or use of administrative tools	Access control logs from central directory stores, as well as network traffic to exfiltrated user databases for offline cracking/ decryption	Unusual access and/or use of systems, outbound access to C2 servers	Large volumes of encrypted data flowing out of the network to suspicious destinations, as well as unusual transaction patterns/ authorizations	Use of secure erasure tools, gaps in log files

Key challenges

Cyber risk is different than traditional IT risks and presents a unique set of challenges:

- The lead time in detecting attacks can be significant due to blind spots and the advanced techniques used by attackers to hide their presence
- Traditional prevention and detection methods (such as signature-based anti-virus) won't detect sophisticated attacks, which have been tailor-made for your environment
- Preventative technologies, such as firewalls and various intrusion prevention systems do not prevent your most sensitive information being sent over the internet if the activity is instigated by what appears to be a legitimate user on one of your systems
- Understanding and establishing a baseline of "what is normal" on your network can be challenging, making it difficult to spot anomalous activity, or indicators of compromise, which require further investigation
- The increasing sophistication in the ways attackers gain an initial foothold can make it very difficult to detect attacks in the early stages – such is the sophistication of phishing techniques that it can be almost impossible to spot a malicious email from a real one, making it difficult to educate your organization's people on how to spot an attack

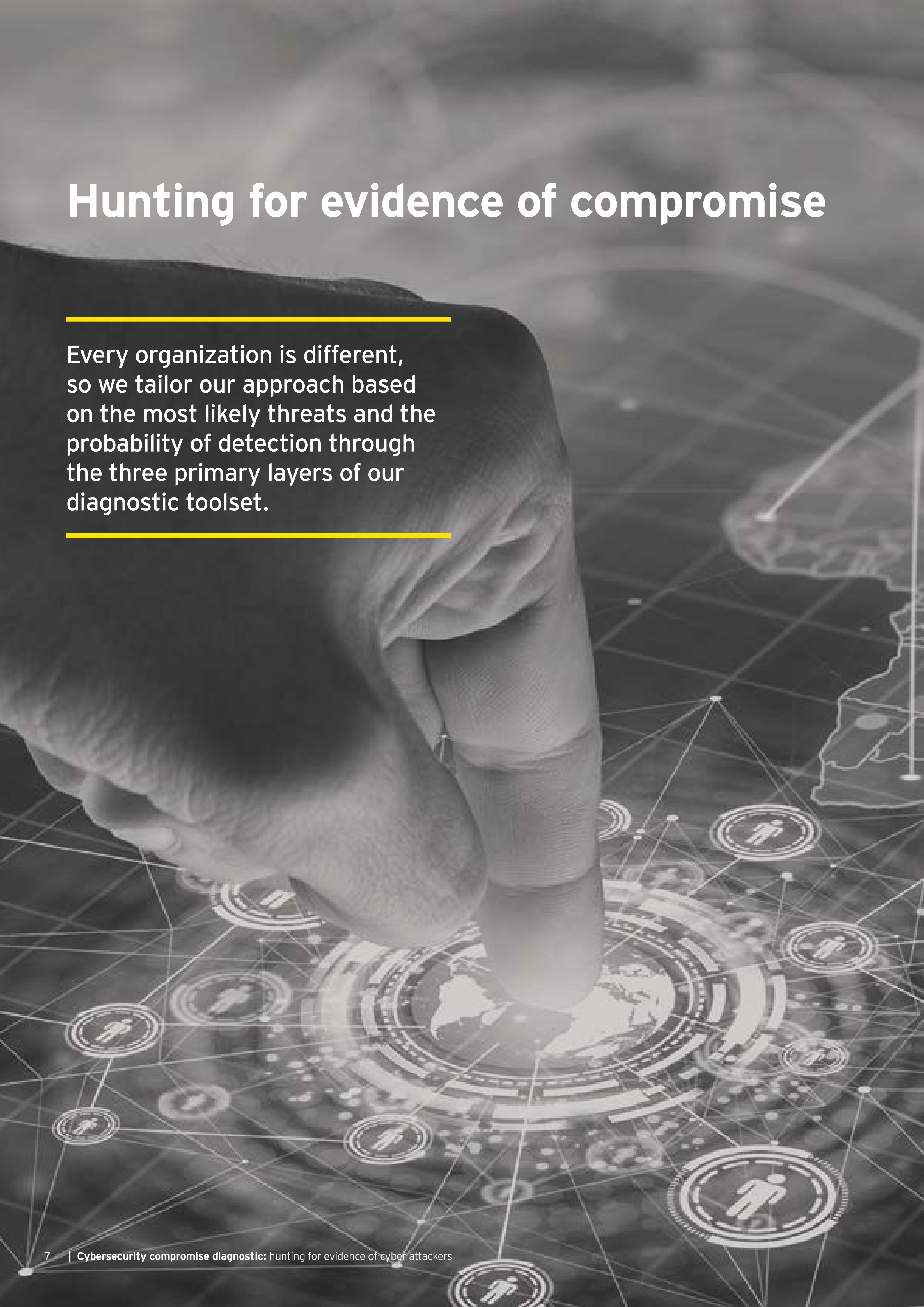
> It can be difficult for cyber defense teams to take the time required to take a step back from routine activities and really focus on determining if there is any evidence on their systems that would suggest they have been, or are currently, subject to a sophisticated cyber attack.

Where to start

Attacks often go undetected for weeks, months, and in some cases, years — by which time the damage is done. The critical first step is determining that your organization has been breached. Given the advanced nature of the attacks and their discrete techniques, an effective way to detect a historical, ongoing or imminent attack is by proactively hunting for evidence of attackers on your systems and networks.

Many organizations don't have a fully-fledged security operations center (SOC) with 24/7/365 security monitoring and response. Those that do often either don't have the right tools deployed in the right locations, or do have tools deployed but have not taken the time to tailor and fine-tune them to their unique environment.

> Organizations setting out on the journey to build a SOC and the supporting tools can get a significant head start by temporarily deploying a highly skilled team with best-in-breed technology to perform a time-limited exercise to understand the tools, while also undertaking an initial hunt for evidence of cyber attackers.



Hunting for evidence of compromise

Every organization is different, so we tailor our approach based on the most likely threats and the probability of detection through the three primary layers of our diagnostic toolset.

How EY can help

Organizations need to adapt and adopt a new detection and response strategy focused on detection through proactively hunting for evidence of attackers on their own networks and systems. EY has developed the cybersecurity compromise diagnostic to help organizations identify signs of compromise, such as that from malware or APT attacks, leveraging leading methodologies and tools.

Our experience shows that organizations understand the need for effective cybersecurity, but are aware that such controls and technologies alone cannot entirely eliminate the threat. Often, network security appliances are put in place to detect intrusions and monitor data leakage. These are used to fend off widely known threats, but are not in themselves a viable defense against a motivated attacker.

IT managers can quickly find themselves overwhelmed with vast amounts of security log data that is never cross-matched or effectively reviewed and prioritized. There are also very few systems that can look below the surface of an organization's IT landscape to uncover the forensic tracks that remain obscured to an attacker.

When breaches are discovered, they are often remediated immediately without executing a full investigation into the attack. This can leave other parts of the network compromised and exposed, as the full extent of the breach is never uncovered. What is clear is that IT and risk personnel need to consider how to protect their IT systems from cyber criminals, but must also consider:

- How to determine whether attackers have slipped past the security defenses
- What can be done if they have

We believe that a proactive approach will help your organization respond to complex incidents that may have breached your security. This can help reduce the amount of time a network is exposed, mitigate the damage or data loss that results and increase the probability of catching the perpetrator; helping to:

1. Detect compromised systems within the organizational environment
2. Evaluate the effectiveness of the current cybersecurity controls
3. Assist with responding to discovered threats
4. Raise user awareness and ability to handle targeted attacks

The diagnostic helps address the threat of hosts within your network being compromised, using market-leading technology to detect suspicious processes and/or, traffic generated by hosts in your network. With the use of the technology, we can detect tailored malware being downloaded onto hosts within your network and analyze suspicious traffic to the outside world in order to identify compromised machines.

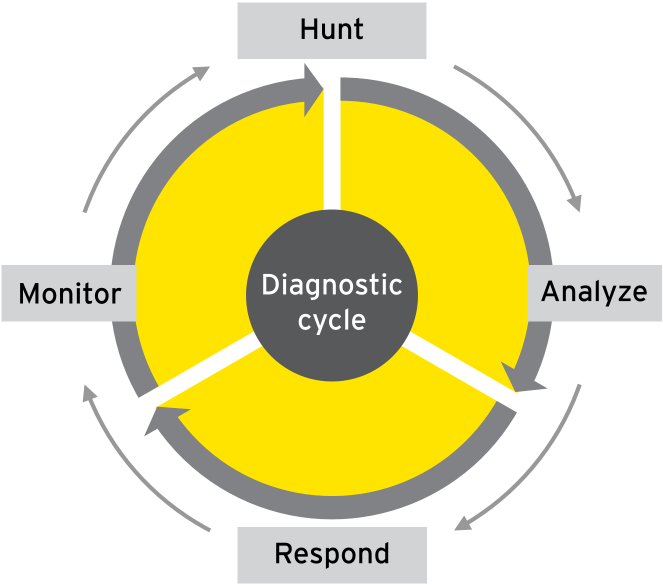
Once indicators of compromise (IOC) have been established, we will report this to you and propose next steps. If desired, EY can assist you with further follow-up and perform forensic investigation activities.

Our approach

We start the **hunt** by understanding the network and systems architecture in place coupled with leveraging cyber threat intelligence to develop a deep understanding of who might be attacking you and why, and most importantly how they might do it.

Using a combination of the methods described below we then **analyze** suspicious activity, assist the organization in **responding** to it and then perform follow-up **monitoring** to detect anything that remains.

We leverage advanced malware detection solutions that identify hosts compromised by threat actors and/or actual and attempted host infections. Through dedicated professionals, we perform APT scanning, discovery and analysis by inserting our monitoring tools at key egress point(s) – we silently scan your network and systems (with little-to-no impact on network performance) looking for suspicious activities that might be a sign of compromised systems. We utilize prebuilt policies to identify and review suspicious network traffic and we can also leverage external threat feeds and feeds provided by you. Custom rules can also be developed, based on bespoke threat intelligence sources.



Every organization is different, and so we tailor our approach based on the most likely threats and the probability of detection through the three primary layers of our diagnostic toolset:

- **Network traffic –** This involves placing a series of sensors at key points throughout your network (typically at egress points and key lateral movement points) to monitor network traffic (typically through a mirrored port or network tap). Alerts and traffic data are sent to a central management console and are analyzed for anomalous events and patterns, applying EY's proprietary intelligence.
- **Host activity –** This entails temporarily installing a low-footprint endpoint agent on selected high-priority systems (typically up to 40,000 systems). The agent reports endpoint activity to a central management console (approximately 1MB of data per day per agent) and is analyzed for anomalous events and patterns applying EY's proprietary intelligence.
- **Targeted analytics –** This approach takes a deeper dive by selectively collating logs and other forensic artifacts from selected high-priority systems, user endpoints and applications, as well as other operating system artifacts where we know evidence of breaches typically reside. Logs are aggregated and then analyzed for suspicious activity, such as compromised user accounts, malicious or persistent code, data exfiltration, etc. We employ a variety of manual and automated tests, user behavior analytics, data mining technologies and the experience of our teams to highlight indicators of suspicious activity, including internal and external access, as well as lateral movement.

We typically adopt a hybrid approach, leveraging one or more of the approaches outlined above in order to increase the likelihood of detecting unwanted behavior. Monitoring is usually carried out over a 4- to 12-week period in order to establish a baseline and identify suspicious traffic after that.

Suspicious activity and artifacts are reviewed by the engagement team and escalated to you once determined to be suspicious or potential incidents, allowing them to be investigated immediately.

We provide a detailed report setting out the assessment undertaken, any findings, and recommended remediation actions. We also provide recommendations on to how to prevent similar compromises from occurring in the future. We typically map any evidence of compromise to the kill-chain, identifying the systems compromised and mapping control weaknesses and suggested improvements along the way.

While leading edge tools are a key ingredient of our approach, they are rarely effective without the skills and experience to use them.

Once deployed, we set about customizing rules and performing manual analysis to root out what's really happening on your networks and systems.

49%

doubt that they are going to be able to continue to identify suspicious traffic over their networks.

57%

of responders have had a recent significant cybersecurity incident.

Statistics sourced from
http://www.ey.com/gl/en/services/advisory/ey-global-information-security-survey-2016

Getting ahead of the attackers

The majority of successful cyber breaches are the result of a multiphase attack that can be mapped to a cyber attack kill-chain. Depending on threat actor sophistication and the organization's defenses, these attacks can take from hours or months to execute. Key to reducing the impact of an attack is to detect it early and take immediate action to shut it down.

For organizations that do not have a full or sophisticated security monitoring capability, performing a cybersecurity compromise diagnostic is the first step to catching the attackers who may already be in, while at the same time giving your organization a hands-on introduction to what a mature security monitoring capability involves. It helps answer questions such as:

1. Is there a threat actor currently operating on our network?
2. How well prepared are we to detect a threat?
3. How can we best respond to and manage discovered threats — what are the specific actions we should take now to secure our systems?
4. How can we raise awareness among our user population and response teams on how to manage sophisticated attacks?

Our diagnostic typically allows us to identify further work streams for investigation. For example, threat indicators might include:

- Evidence of the use of remote access software from unauthorized sources
- Indicators of the presence of active malware
- Persistent connections to other countries or unauthorized entities
- ''Back channel'' data flow into and out of your organization
- Indicators of data harvesting by employees or leavers
- Unauthorized system and data access

In addition to these indicators, we often uncover other findings that relate to your IT security or information governance regime, including:

- Limitations of existing security policies
- The storage of confidential data in unprotected areas (webmail, cloud storage, etc.)
- Inappropriate use of IT resources
- Misconfigured network devices
- Installation of unauthorized software or hardware

The output of our analysis will likely be the identification of a number of issues that can be passed directly to an IT remediation or investigation team. These issues should be prioritized according to your objectives and the perceived severity of the threat. For example, you may allocate internal IT resources to the mapping and eradication of a seemingly innocuous botnet. Similarly, you may instruct an in-house forensic team to investigate indicators of a possible internal data theft.

Clients are often reluctant to let us leave at the end of a successful diagnostic project. This is certainly not because we don’t finish the job, but because they don’t want to give up the deep monitoring capability we provide during the project.

Quite often, a cybersecurity compromise diagnostic leads to a longer-term initiative from our clients to help them build their own security monitoring capability.

Why EY?

We work with many of the world's leading businesses on their cybersecurity journeys, both assisting them with proactively building capability and also through their most difficult times — when they have suffered a cyber breach.

EY has developed an approach to sampling networks for indicators that a breach may have occurred. This is in contrast to a traditional IT audit or a vulnerability test, which focuses on potential weaknesses to common, well-publicized attacks. Our cyber security compromise diagnostic focuses on those targeted attacks that are designed to slip past your defenses

- **Close collaboration —** We work closely with you to support your cybersecurity teams to understand and respond to sophisticated attacks. We believe that substantial knowledge transfer is vital in these types of projects, so that you take away more than just our report. A cybersecurity compromise diagnostic is similar to a vulnerability assessment, insofar as it should be undertaken at regular intervals. We can help you take this process in-house.
- **A strong team —** EY teams bring deep experience serving a variety of industry sectors with a specific focus on information security, cyber risk and cyber incident response. Our subject-matter advisers will also provide challenge and validation of cybersecurity scenarios such as data loss, loss of data integrity, APT and DoS attacks, or a combination thereof.
- **Extensive security operations experience —** We work with our clients to design, build and then operate their SOCs, including the core capabilities of cyber threat intelligence, security monitoring and incident management. We bring this experience to every cybersecurity compromise diagnostic assignment, meaning that clients who are starting on their SOC journey can leverage our broad experience.
- **Understanding of cyber threats and resulting issues —** We have a current, in-depth and extensive knowledge of global cyber threats and related cyber incidents, the wider information security and cyber risk landscape, challenges faced by our clients and experience in forensic investigations. We bring our knowledge of the industry threats in each sector we operate in, coupled with specific threats that impact our clients' organizations.
- **Leading-edge tools and techniques —** We leverage leading class tools, techniques and quality controls. We are technology agnostic, meaning that we'll provide you with access to appropriate tools for the job, giving you the opportunity to witness them in action on your own systems.
- **A strong track record in performing these diagnostics —** EY teams have supported clients globally in these diagnostics, including global banks, regulators in Europe, the Middle East, India, Africa and the US, insurers in the UK, stock exchanges, aviation organizations, government, manufacturing, retail, distribution utilities and oil and gas organizations.
- **Experience in responding to multiple breaches —** We have decades of experience in assisting our clients' response to a large variety of cyber breaches. We know how to respond and stop a sophisticated attack in its tracks.

wavespace™

EY has launched its global network of growth and innovation centers to help clients make radical breakthroughs in business transformation by tapping into innovative thinking.

The EY wavespace™ global network brings together multidisciplinary talents, unique capabilities and IP, in collaborative, interactive working environments. We focus on disruptive growth, improvement strategies and technologies that impact specific industries.

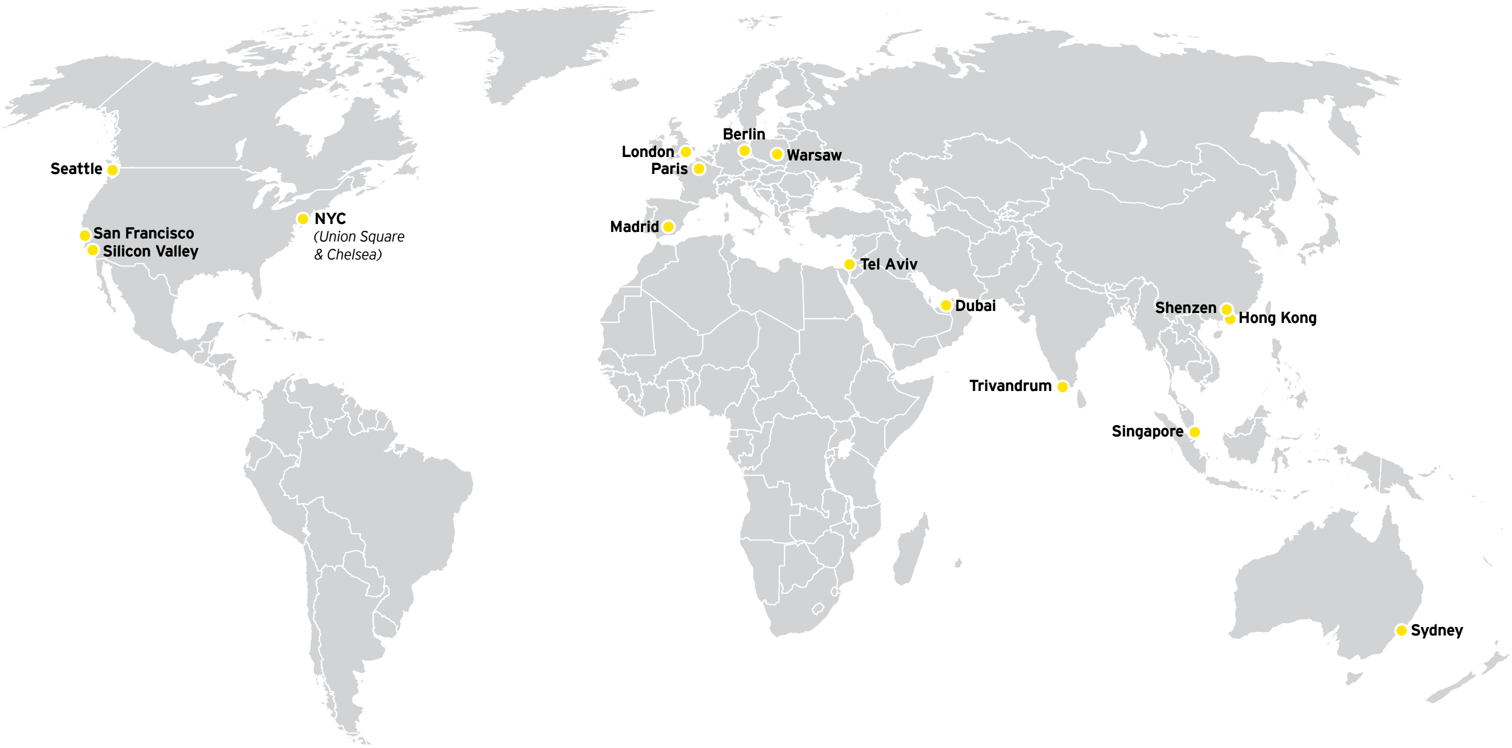
The wavespace™ centers expand EY's existing network of innovation centers. These were developed to help clients face the challenges and opportunities of continuous change, digitization and disruption in the transformative age.

wavespace™ locations feature a shared methodology and platform that combines EY's experience in disruptive technologies, such as artificial intelligence, robotic process automation (RPA), blockchain, data analytics, digital, customer experience and cybersecurity, with EY's deep industry domain and regulatory experience.

Our flagship wavespace™ locations have room for up to 150 multidisciplinary teams working across digital, analytics and cybersecurity in one physical space. Housing design studios, technology incubators and real-world showcase centers, each location is designed to deliver impactful, relevant experiences along with highly effective collaboration sessions aimed at developing immediately actionable opportunities. And wavespace™ is more than just a physical place, it's a state of mind. It can help clients capitalize on disruption and think differently in order to ask better questions which help them build a better working world and thrive in the transformative age.

In a multimillion dollar investment, EY will increase its current network of 16 flagship wavespace™ locations by adding centers in the Americas, Europe, the Middle East and Asia-Pacific. Each wavespace™ locations features dedicated multidisciplinary teams who can help clients successfully navigate the transformative age and discover new ways of creating value. These complement our growing network of satellite centers that maintain capabilities across artificial intelligence, RPA, blockchain, data analytics, digital, customer experience and cybersecurity.

We're stronger when we're connected. Understand how to thrive in the transformative age by exploring innovative new ideas and asking the questions that build a better working world at one of our global wavespace™ locations. The future belongs to the connected.



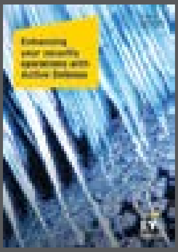
Want to learn more?

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.

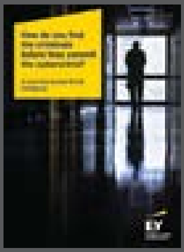
Please visit our Insights on governance, risk and compliance series at ey.com/GRCinsights.

Further information is available at: ey.com/cybersecurity

Path to cyber resilience: Sense, resist, react
EY's 19th Global information Security Survey 2016-17



Active Defense:
Enhancing your security operations with Active Defense



Cyber threat intelligence:
How do you find the criminals before they commit the cybercrime?

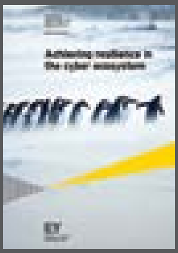
Security Operations Centers:
Helping you get ahead of cybercrime

Third generation SOC:
Using cyber analytics to help you get on top of cybercrime

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

Cybersecurity and the Internet of Things

Incident response
Preparing for and responding to a cyber attack



Achieving resilience in the cyber ecosystem

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.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization and may refer to one or more of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no: 04702-173GBL
28573.indd BSC (Ireland)

ED None.

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

For questions about cybersecurity, please contact EY cybersecurity leaders:

Global

Paul Van Kessel
+31 88 40 71271
paul.van.kessel@nl.ey.com

Americas

Bob Sydow
+1 513 612 1591
bob.sydow@ey.com

EMEIA

Mike Maddison
+44 207 951 3100
mike.maddison@uk.ey.com

Asia-Pacific

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

Japan

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

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.