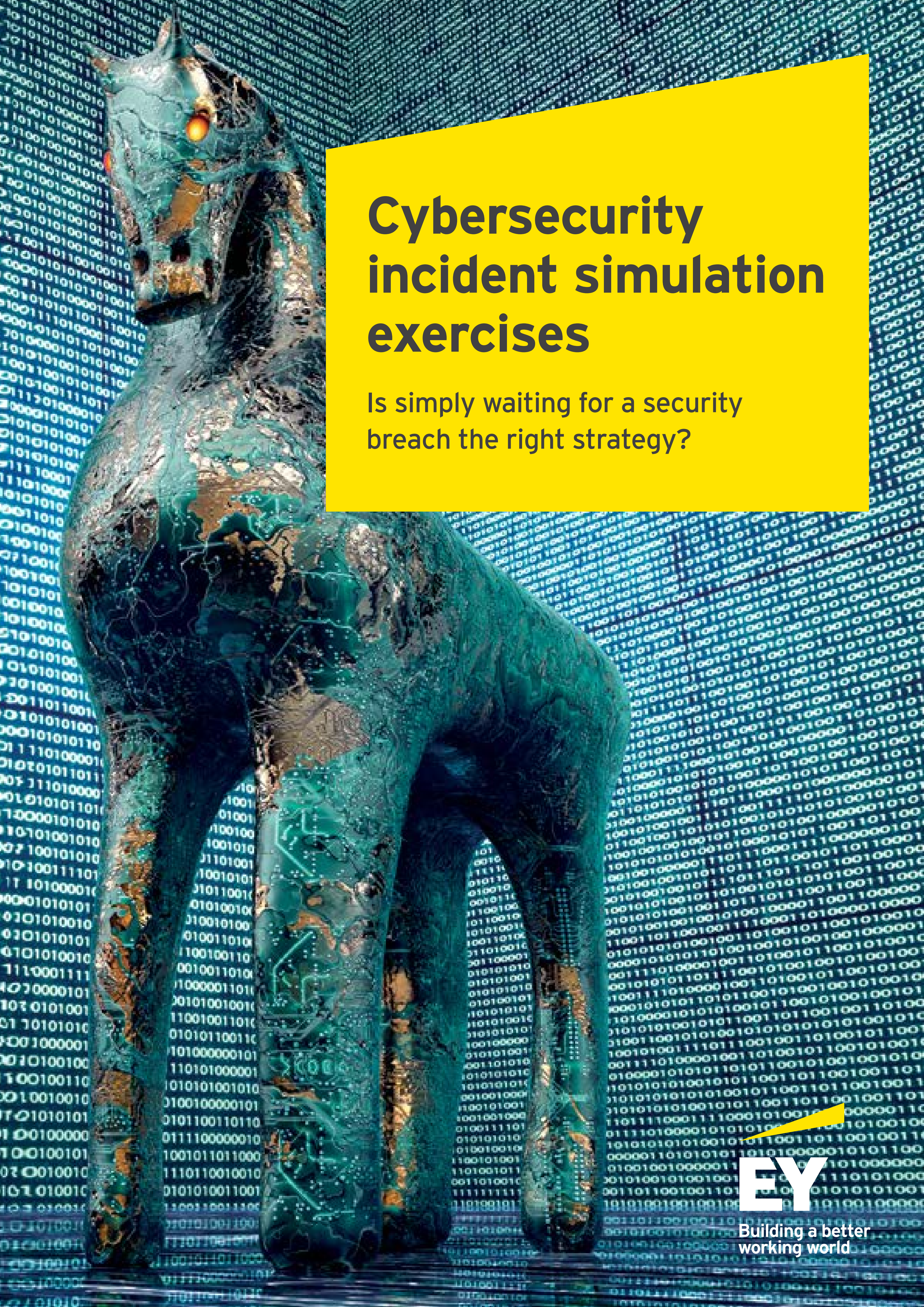
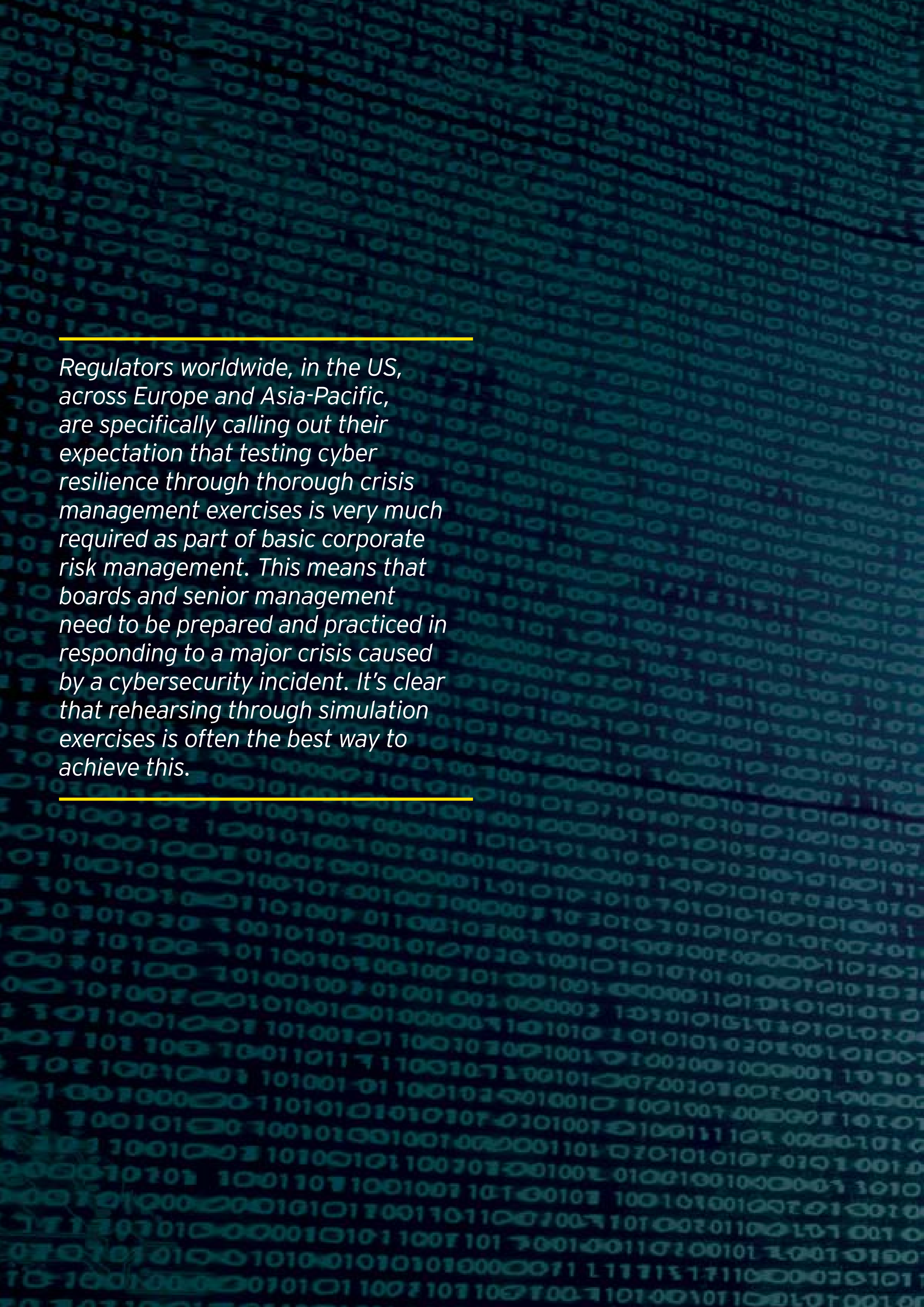


Cybersecurity incident simulation exercises

Is simply waiting for a security breach the right strategy?

Building a better working world

Table of contents



Regulators worldwide, in the US, across Europe and Asia-Pacific, are specifically calling out their expectation that testing cyber resilience through thorough crisis management exercises is very much required as part of basic corporate risk management. This means that boards and senior management need to be prepared and practiced in responding to a major crisis caused by a cybersecurity incident. It's clear that rehearsing through simulation exercises is often the best way to achieve this.

Preparing for the inevitable

A response plan that has not been tested is as useful as having no plan at all.

The midst of a cybersecurity incident is not a good time to test the plan.

Scenario-based testing of your cybersecurity incident response capability is a high-impact way of engaging your response teams (which includes executive leadership and not just the IT team) in the business decision-making process that goes with reacting to a critical incident. Regular testing of your response plans will help everyone involved to be familiar with the process and prepare them to react when a critical incident occurs.

How would you respond?

The race to a digital world, and the inherent connectivity of people, devices and organizations, has opened up a whole new playing field of cyber risk. We now have an irreversible reliance on technology in all aspects of our lives and the line between personal and business use continues to blur — we're all in the cloud, whether we like it or not!

Businesses are focusing their strategy on new digital channels to maintain a competitive edge, while consumer-driven Internet of Things (IoT) developments create brand new benefits and risks for digital citizens, including connected cars, medical devices, critical infrastructure, and even smart cities.

Hardly a day goes by without reports of another high-profile cyber attack hitting the headlines. Organizations frequently fail to manage the response, and in our experience, this can be more damaging than the fact that they suffered a breach in the first place. It can suggest that not only were they breached, but they were not in control of the situation either.

Cyber risk is now one of the most commonly talked about topics as the impact of cybercrime reaches an all-time high. There are high expectations from institutions, markets, regulators and the public for organizations to protect themselves and their customers at all costs. It's no longer a question of if your organization will be breached, or even when, it's likely to have happened already. The real question is do you know and are you prepared to react?

A shift in mindset

Accepting today's reality is the first step:

- There are only two types of organizations: those that have been hacked and those that will be.
- It is a real challenge when organizations do not realize they have been breached, and fail to react in a planned and coordinated manner.

Organizations typically overlook the importance of rehearsing the time-pressured technical, process and business decision-making that is a critical component of being prepared to respond to a cyber attack.

Those who fail to prepare will struggle to contain an attack and will feel the impact to a far greater extent. Having a cybersecurity incident response process that manages an incident from identification through investigation, containment, remediation and follow up is the first step. Being fluent in how to use it is vital. Simulated events are an excellent way to achieve this fluency, which is a key part of any resilience program.

Testing all aspects of the cybersecurity incident response can be complex, requiring the right level of challenge to the different capabilities involved in an effective response. The composition of an organization's incident response team varies greatly, with some smaller organizations having a single team, and others having separate teams to address technical detection and response, managing the incident response process, and executive decision-making. The different skillsets, internal and external dependencies, and the organization's approach to incident management, further emphasize the need to explore cybersecurity incident response before responding to a live incident.

> *The focus is no longer prevention: you can't stop attacks.*
>
> *It's now about better detection and readiness for the inevitable in order to survive in today's complex world.*

Key challenges

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

- Cybersecurity incidents are high-speed, unstructured and diverse — crisis management for these cases is intense and demanding
- Unlike one-off incidents, motivated attackers mount persistent dynamic campaigns, with the scale and complexity of threats continuously expanding
- The impact in terms of both cost and reputational damage can be severe
- Every organization has a broad range of entry points, including third parties and internal staff
- Traditional business continuity management (BCM) typically focuses on availability of systems and data — this may be ineffective, for example when data integrity issues are replicated automatically across disaster recovery (DR) systems
- Keeping current and well-versed across people, process and technology response capabilities, and across technical, project management and executive management teams can be difficult in the face of competing priorities
- Obtaining executive buy-in and participation in incident response planning and exercises can be difficult if the risks are not well understood
- Shortage of skills and internal capability to respond to an increasing number of complex attacks can leave organizations exposed
- Organizations frequently learn of a cybersecurity breach from outside sources, such as law enforcement, a regulator or a client, and struggle to keep control of the incident
- Managing the media when the news of a security breach has already gone viral and is being discussed by your customers on social media and other channels outside of your control
- Assuring customers, regulators, investors and other interested parties that the breach is under control
- Engaging with regulators to demonstrate proactive incident management capability (e.g., minimizing financial impact and ensuring the protection of customer information)

> *Heavily connected industries, such as financial services and critical national infrastructure (CNI) pose a systemic risk to the markets they serve.*
>
> *We are now seeing national cybersecurity incident simulation exercises being carried out by governments and/or industry associations, such as the Waking Shark exercises pioneered by the Bank of England and similar by SIFMA in the US.*
>
> *This helps to exercise the reaction to cybersecurity incidents, which impact various parts of the supply chain, from financial transactions to the operational technology that underpins our daily lives.*

An effective response

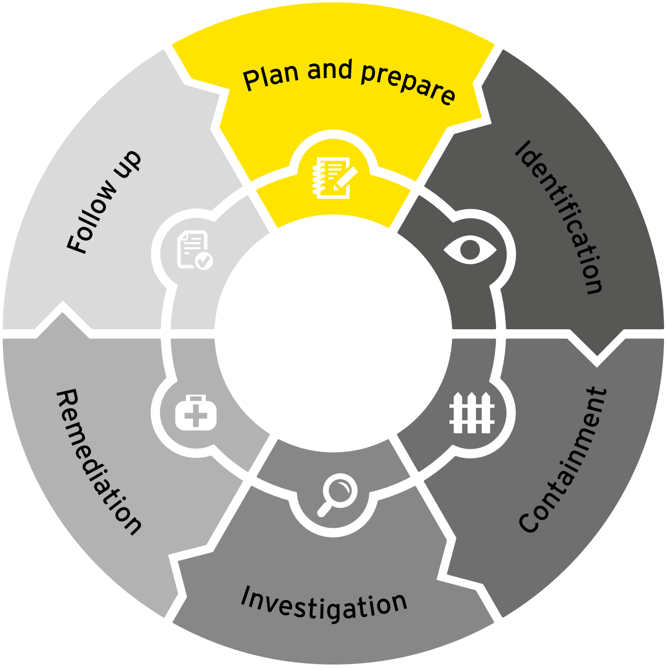
Every attack is different, and so is every organization. The typical response process, based on leading practice, is outlined here — however, to be effective, an organization must have a response plan that is tailored to it.

Areas specific to an organization include: its critical assets, the threats most likely to be realized, its identification and detection processes, decision-making criteria and reporting lines, in addition to team members and underlying technologies. Identifying and engaging with third parties (both those involved in regular business with the organization and those, such as law enforcement and specialist lawyers, who are required in the event of a breach) is of vital importance.

Advanced organizations leverage cyber threat modeling to not only identify the top threats, but also prepare responses and countermeasures ("play books") to these.

While every incident is different, a typical response plan follows a structured approach. This starts with detailed planning and preparation, which includes testing capability through simulation exercises. Once an incident is identified, it is triaged (categorized and classified) and initial steps are taken to contain the impact. An investigation into root cause is commenced and, once possible, steps are taken to remediate the issue and bring the organization back to a stable state. A key step that is often skipped is following up after the incident with lessons learned to enable long-term improvements in both the response process and the organization's ability to sense, resist and react in future.

The capability to react rapidly to a cyber attack helps to minimize the possibility of long-term material impacts. Organizations that develop superior, integrated and automated response capabilities can activate non-routine leadership, crisis management and coordination of enterprise-wide resources quickly.



A response plan solely focused on and run by IT is destined to fail. An effective response involves all aspects of the organization, from the CEO, to HR, general counsel, media relations and IT, among many others.

How EY can help

Organizations that have a robust response capability in place, and one that is regularly tested, are at a significant advantage when it comes to reducing the impact of a cybersecurity breach. A proven way to refresh your capability to sense and react to cyber attacks is to proactively prepare via cybersecurity incident simulation exercises. This helps identify whether roles, responsibilities and protocols are fully understood by all parties in a practical real-world manner, in addition to helping identify which threats are most relevant to your business. Some key characteristics are:

- Exposure to cyber threat actor motivations
- Reacting in a timely manner to fast-paced events
- Awareness of the impact on customers
- Engaging with third parties that may be the cause of, or impacted by, a cybersecurity incident
- Internal and external communications strategies
- Some technical aspects of a cyber attack
- Pressurized decision-making based on incomplete information
- Availability and effectiveness of external support (technical/forensic specialist) and mitigations (cyber insurance)

Every incident is unique and so is every organization. At EY, we invest significant effort in tailoring each scenario to reflect the latest threats our clients face at the time of the exercise, in addition to providing a robust challenge in a client-specific environment.

We typically provide cybersecurity incident simulation exercises designed to challenge audiences at various levels. A sample of the exercise types is outlined here, however, more often than not, we produce tailored exercises involving a mixture of elements from multiple exercise types. We frequently work with our clients to develop a multiyear plan that involves a variety of exercise types at different levels to really stress test the full response capability, from boardroom decision-making through to technical investigations teams.

Industry-wide exercises are something EY is specifically familiar with. Rather than wait for regulators to come knocking, we are seeing more and more industry associations take the lead and organize multi-stakeholder exercises, specifically designed to challenge systemic risks in complex supply chains.

Executive cybersecurity incident simulation exercise

- **Exercise description –** This highly engaging, interactive and immersive exercise typically lasts a half day and is focused on the unique executive-level decision-making and communication strategies that are critical to any crisis response. In a safe environment, participants are able to truly experience what it is like to respond to a sophisticated cyber attack, increasing their level of awareness and gauging their readiness to manage a cybersecurity incident. Participants typically discuss the actions they would take without necessarily implementing them.
- This highly customizable exercise typically presents the participants with a number of initial pieces of information related to the potential cybersecurity breach. In the preparation of the exercise, organization-specific scenarios are typically created based on current threat intelligence. Throughout the session, the situation further unfolds, driven by the actions of the participants, as well as inputs from traditional and social media alike.
- **Options –** A range of options can be selected and combined in order to tailor the exercise to organizational objectives. We can conduct the exercise as a formal test through selecting predefined scenarios and providing guided reflection and facilitated discussion throughout. The exercise can also be played as a highly dynamic game, drawing on gaming elements, such as action cards, custom-built applications (including live media feeds) and actors providing real-time feedback in the role of media and stakeholders.
- **Primary objectives –** This exercise has proven to be an effective catalyst to trigger cyber risk conversations at board level as participants experience first-hand how to assess, decide, engage and communicate during a cybersecurity crisis. The exercise may aim to increase awareness, or to have more formal objectives to provide evidence of cyber resilience to regulators. This can include testing the ability of executive management to make decisions during a crisis, in addition to incident coordination at a high-level.
- **Target audience –** C-suite (CEO, COO, CRO, CFO, CTO, CIO, CISO), board members, general counsel, PR/communications, HR, business units, cyber threat intelligence, business continuity management, and incident coordinator (however not the full incident coordination team).

Incident coordination simulation exercise

- **Exercise description –** This exercise typically lasts a half day and focuses on challenging the incident coordinator and their team as they execute their response plan. Participants perform all, or the majority of, the processes documented in the plan. (Participants may discuss the actions they would take without necessarily implementing them.)
  The exercise is customized to the organization and their incident management plans and typically involves providing participants with a series of customized injects that challenge their ability to coordinate their response at both the strategic and tactical levels.
- **Options –** The exercise can be customized to include testing technical elements in a desktop-based manner. Elements of gamification can also be added.
- **Primary objectives –** To test the ability of the incident coordination team to manage the incident through to its conclusion, including interacting with the executive-level team.
- **Target audience** – CTO, CIO, CISO, incident coordinator, incident response lead, investigations lead, cyber threat intelligence, business continuity management and technical professionals.

Response team simulation exercise

- **Exercise description** – This exercise can last from 1-2 days to 6-8 weeks and really gets hands-on from a technical perspective, challenging an organization's ability to sense and react to sophisticated attackers. Following detailed planning and establishing rules of engagement, EY's Red Team conducts active attacks against the organization that should be detected and responded to by security monitoring and response teams. Participants undertake the technical actions they would do to defend and eradicate the threat. The exercise typically involves a series of social engineering/external penetration activities to gain a foothold, followed by internal lateral movement and escalation of privileges in order to access trophies – all while avoiding detection.
- **Options** – There are three typical approaches we take to these dynamic exercises:
  - **Technology-enabled simulation –** A scenario is agreed in advance and leverages prepositioned internal and external systems to execute scripts that emulate attack scenarios.
  - **Purple Team exercise –** Predefined scenarios are jointly developed by EY's Red Team and the client's Blue Team and executed together, allowing live collaboration, which drives communication and coordination.
  - **Live war game –** EY's Red Team develops and executes predefined scenarios without detailed collaboration with the client (basic rules of engagement and target trophies are agreed), allowing the client's Blue Team to react in real time - all the time observed EY.
- **Primary objectives** – Test the security monitoring and incident response capabilities of the organization's security operations center (SOC).
- **Target audience** – CISO, incident coordinator, incident response lead, investigations lead, technical professionals, cyber threat intelligence, and security operations (this may be extended to include the full incident coordination team, depending on objectives).

Our approach

For many of our clients, we develop a tailored exercise that is a hybrid of exercise types. We adopt a streamlined approach to developing each customized exercise so that it provides a realistic scenario that really challenges.

Our approach is to provide a condensed and very intense exercise to simulate a critical cyber attack. During this time there are multiple events occurring that impact the organization. These injects are presented within the exercise using a variety of methods. The participants must consider all information received, assess, understand and prioritize it, and take appropriate actions if pertinent. As the exercise unfolds, the complexity increases so that key activities can be assessed and areas for improvement identified. As standard, the exercises assess how the team responds to each challenge, and keeps focused on key areas, the approach taken, methods applied, and the effectiveness of decision-making and communications.

Key challenges in providing simulated events include maintaining a sufficient level of reality, coupled with compressing time. We invest significant effort in developing highly customized scenarios that have been vetted to confirm that they "could happen" to the client. For our nontechnical exercise types, we ensure that there are no dependencies outside the exercise team that could slow events down and/or distract from the primary objectives of the exercise. This is a vital success factor, as any exercise would quickly lose impact if it were necessary to wait for an answer from outside the exercise team. While this is not inline with reality, it is necessary to get the most out of the time invested by the various teams in the exercise.

There are a number of additional options that we frequently provide:

- **Coaching –** an experienced team coach provides a more thorough assessment on team dynamics, interaction within the group environment and individual responses to challenges.
- **Media workshop –** an external crisis media specialist facilitates an interactive workshop focused on crisis management do's and don'ts from a media perspective.
- **Framework review –** perform a design effectiveness review of the existing cybersecurity incident response plans/procedures and provide recommendations for improvement. This is typically followed by a series of workshops/training sessions to facilitate success the next time they are tested.

Critical to the success of any exercise is that it is tailored to the organization and is provided in a highly engaging manner. EY uses a variety of methods to provide a truly immersive exercise, which keeps participants actively engaged throughout. We leverage a variety of techniques, from centralized communications centers, text, video, audio and multimedia experiences to truly replicate how a real crisis would look and feel.

Planning and design

Our detailed customization starts very early in the process. This involves leveraging external cyber threat intelligence to identify the most relevant and likely threats to the organization, both from an overall industry perspective and those specific to the organization. If available, we work with our client's cybersecurity team to understand historical threats and attacks to further focus our simulation scenario development. We work closely with nominated contacts to plan and design an incident scenario and simulation that are realistic and provide the opportunity to assess how your response teams react. This includes defining roles and responsibilities of the exercise team as well as the response team(s).

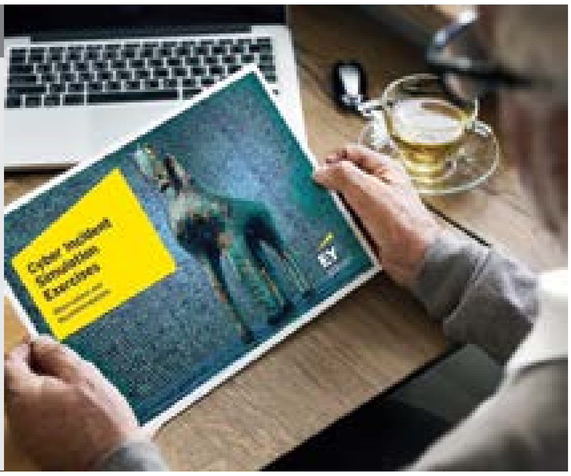
Incident simulation

Following detailed planning and meticulous preparation, our experienced teams facilitate the exercise, typically in the same location that our clients would convene their response teams (the "war room"). Our nontechnical exercises typically span a half-day, which covers a simulated timeline (e.g., 1-3 days), during which the response team(s) practice their responses and we identify areas for improvement.

While we do provide strong facilitation, up to and including "crowd control", the exercise is led by the response team. For technical exercises, we only interject if the exercise is likely to stray outside of the agreed rules of engagement.

Reporting

At the conclusion of the exercise, we typically hold a "hot debrief" to get immediate feedback from the participants, both on the exercise itself, but most importantly on areas they identify for improvement. This is followed up with a written report that provides an overview of the exercise, each inject and the response and decisions from the response team, coupled with our concise observations and recommendations for improvement.



The advantages of being prepared

EY can help challenge your organization's current cybersecurity readiness by taking you through a controlled, simulated cybersecurity crisis. This provides:

- An effective step for management to discuss the broad range of issues related to a crisis scenario
- Quickly identify business risks presented by gaps in current cybersecurity defense capabilities
- A test of the ability to react to multiple, often combined cyber attacks, such as Distributed Denial of Service, cyber extortion, ransomware, data/IP theft, malicious insiders, etc.

Our cybersecurity incident simulation exercises are designed to provide you with a rapid, independent assessment of your current capability to sense, resist and react to a broad range of cybersecurity threats, by simulating one or more cybersecurity incident scenarios.

Depending on the approach taken, benefits include:

- Significant improvement in clarity of roles, protocols, internal communication paths and escalation procedures across the business in the event of a cyber attack
- Individuals that have learned to follow a certain routine during live-tests tend to be much more action-oriented, and with that, more effective in actual crises
- Improves team readiness for a cybersecurity incident response – the team will "have done it before" together, ironing out any issues that arise in a safe environment and "building muscle memory"
- Tangible improvements to your existing response plan and capability — testing people, process and technology invariably identifies areas for improvement that would not usually be detected through a desk-based manual review of incident response documentation

Cybersecurity incident simulation exercises provide robust challenges across a variety of areas, allowing an organization to not only gauge the effectiveness of its response capability, but most importantly, gain experience in a safe environment.

We work with many of the world's leading organizations on these issues and our teams of dedicated security professionals extends to the global network of EY wavespace^{TM} locations. This service is scalable and therefore accessible for small and medium-size enterprises, as well as large global organizations.

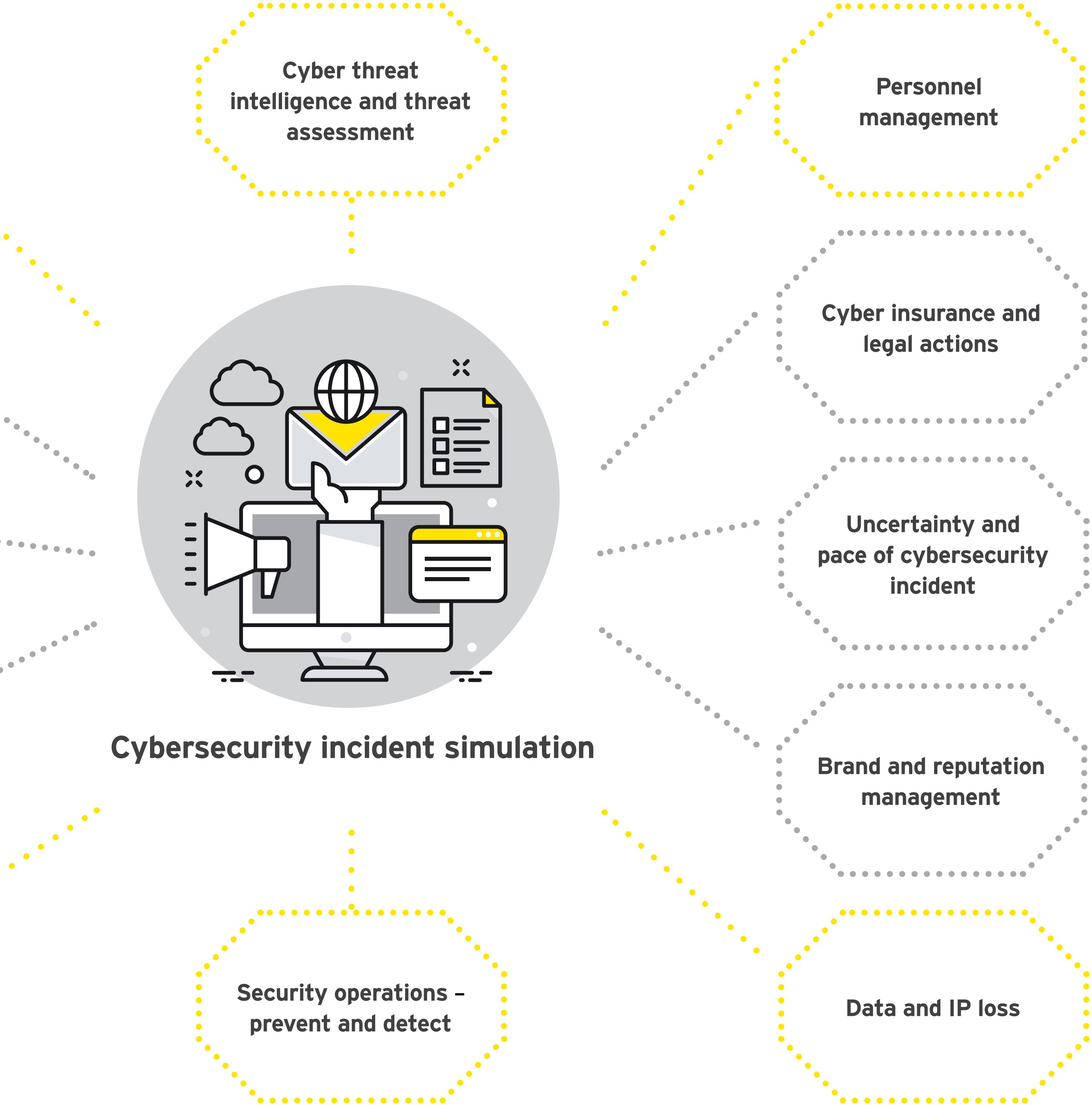
Executive committee cybersecurity knowledge and engagement

Media and communications management

Operational interruption and business continuity

Response team readiness

Regulator interaction



Cybersecurity incident simulation

Cyber threat intelligence and threat assessment

Security operations – prevent and detect

Personnel management

Cyber insurance and legal actions

Uncertainty and pace of cybersecurity incident

Brand and reputation management

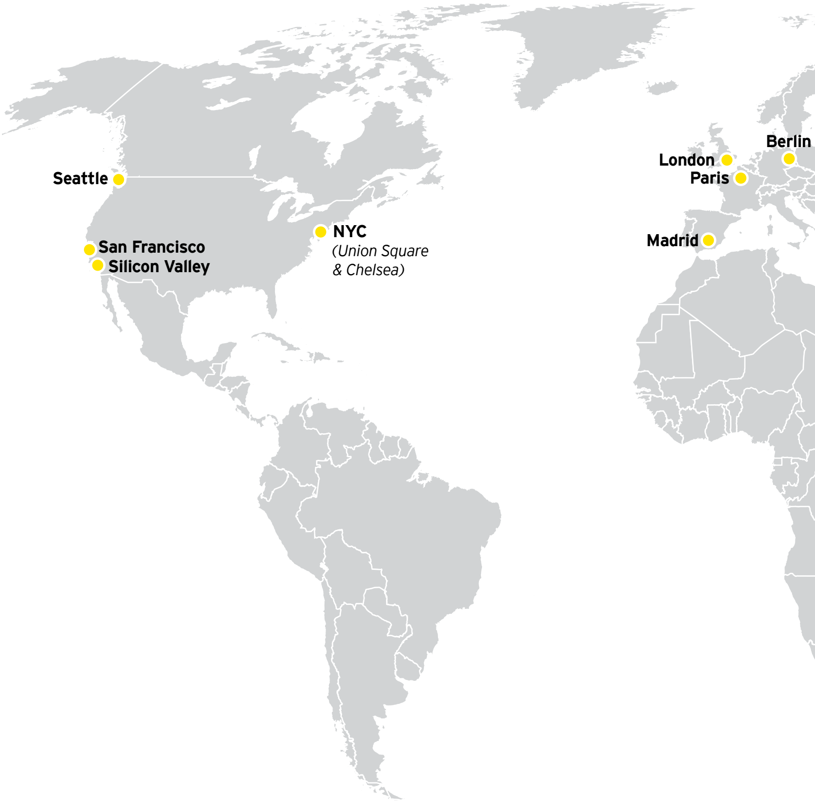
Data and IP loss

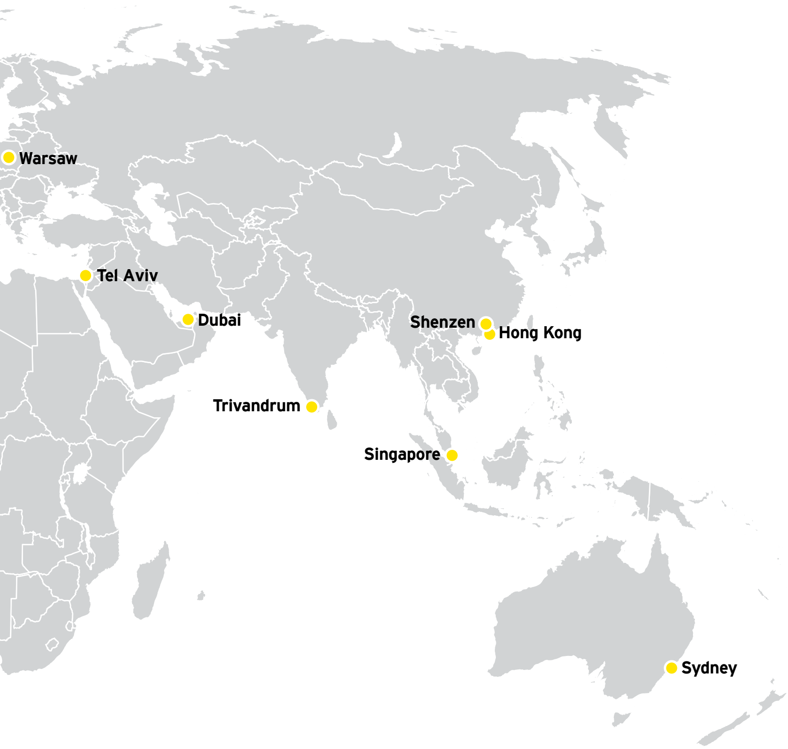
Why EY?

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

- **We see the full picture** — We understand what it takes to build a response capability and to respond to sophisticated attacks. We have done both of these before, numerous times. We take a broad-spectrum approach to developing exercises that are designed to effectively test the various capabilities that combine to deliver an effective response. While one-off tests of individual components can be useful, it's vital that the full response ecosystem is considered from the start.
- **Close collaboration** — We work closely with you to help your incident response team to appropriately respond to cybersecurity incidents by developing a realistic incident scenario with significant impact and provide observations and actionable recommendations.
- **A strong team** — Our experienced teams bring deep experience serving various industry sectors with a specific focus on information security, cyber risk and cybersecurity incident response exercise development. Our subject-matter advisors will also challenge and provide validation of cybersecurity scenarios, such as data loss, loss of data integrity, advanced persistent threat (APT) attacks, denial of service attacks (DoS), etc., or a combination thereof.
- **Understanding of cyber threats and resulting issues** — We have a current, in-depth and extensive knowledge of global cyber threats and related cybersecurity incidents, the wider information security and cyber risk landscape, challenges faced by organizations, and experience in forensic investigations.
- **A strong track record in performing these exercises** — EY teams have supported clients globally in these exercises including global banks, regulators in Europe, the Middle East, India, Africa and US, insurers in UK, US and Australia, stock exchanges, aviation organizations, government, manufacturing, retail, distribution utilities and oil and gas organizations. We have supported our clients with incident simulation exercises for many years with increased focus on cyber risks over the last decade.

Our global reach enables us to seamlessly scale inline with our clients' requirements and global footprints, and the complex business and regulatory environments in which they operate.





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.

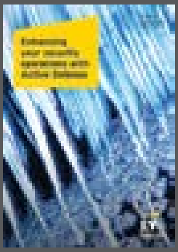
We're stronger when we're connected. Understand how to thrive in the transformative age by exploring innovative new ideas and asking the questions that build a better working world at one of our global wavespace™ locations. The future belongs to the connected.

Want to learn more?

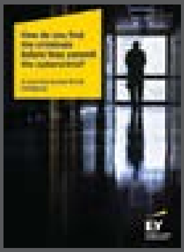
Insights on Governance, Risk and Compliance, is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable 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

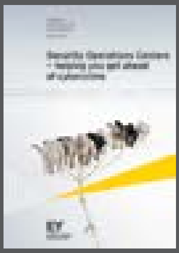


Active Defense:
Enhancing your security operations with Active Defense



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

Security Operations Centers:
Helping you get ahead of cybercrime

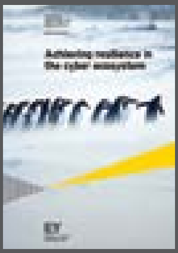


Third generation SOC:
Using cyber analytics to help you get on top of cybercrime

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.

© 2017 EYGM Limited.
All Rights Reserved.

EYG no: 04703-173GBL
25834.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

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.

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