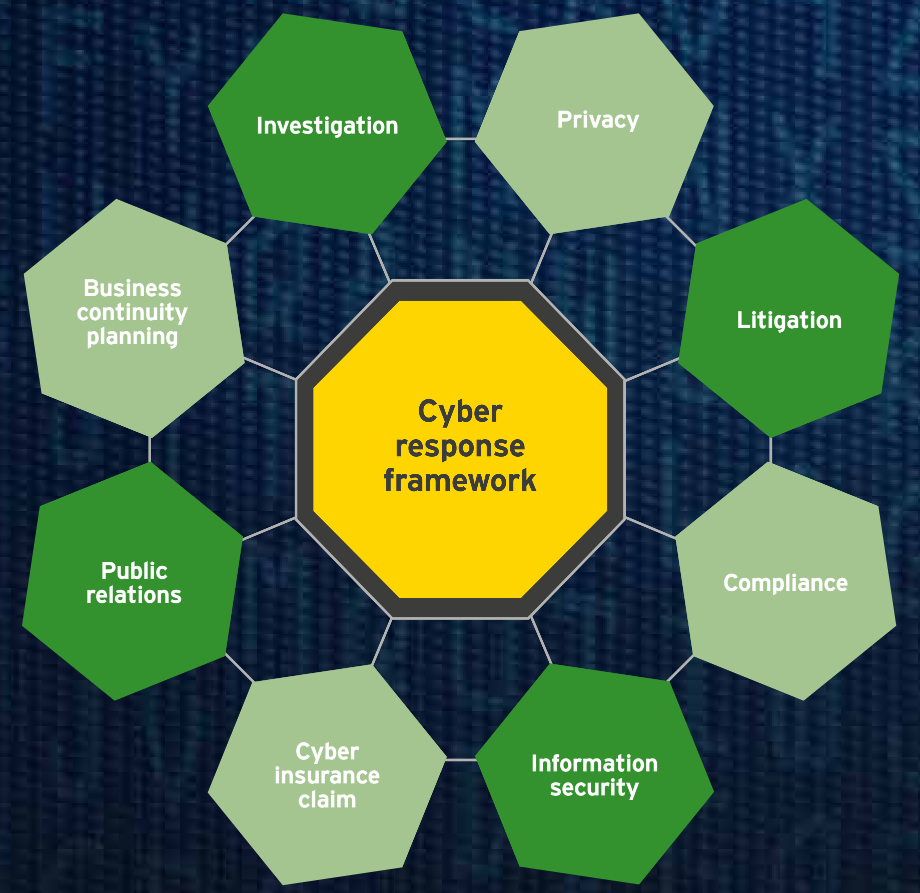
The wide-ranging business impacts and risks of cyber attacks

It is only a matter of time before a business will suffer a cyber attack. The potential impact of cybercrime requires that cybersecurity be viewed as a business risk, rather than a simple IT issue. Fundamentally, an organization's reputation is on the line as a cyber attack may impact business operations, financial integrity, and legal exposure to its customers and partners.

In addition, cyber risk has been increasingly linked to data protection and privacy regulatory compliance around the world. For example, the EU's General Data Protection Regulation (GDPR) that went into effect in May 2018 requires that supervisory authorities be notified, under certain circumstances, within 72 hours of a personal data breach. The EU Network and Information Security Directive incident notification requirements for digital service providers (DSP) dictate that DSPs notify the competent authority without undue delay of any incident having a substantial impact on the provision of a service. China's Cybersecurity Law became the first national-level law that addresses cybersecurity and data privacy protection in November 2017. The United States has approximately 20 sector-specific or medium-specific national privacy or data security laws, and hundreds of such laws among its 50 states and its territories such as the California Consumer Privacy Act of 2018.

In order to adequately address the risks from large and complex cybercrimes that are likely to occur, it is critical that organizations develop a strong, centralized response framework that is part of the enterprise risk management and crisis management strategies.

> "What would once have been considered large-scale cyber attacks are now becoming normal."
>
> ***The Global Risks Report 2018***
> World Economic Forum



Cyber response framework

Investigation

Privacy

Litigation

Compliance

Information security

Cyber insurance claim

Public relations

Business continuity planning

Global presence

	Americas:
🟪	Atlanta
🟪	Belo Horizonte
🟪	Bogota
🟪	Boston
🟪 🟩	Buenos Aires
🟪 🟧	Charlotte
🟪	Chicago
🟪 🟧	Cleveland
🟪	Curitiba
🟩 🟦	Dallas
🟪 🟩	Houston
🟪	Iselin
🟪	Lima
🟪	Los Angeles
🟪	Mexico City
🟪	New York
🟪	Quito
🟪	Rio de Janeiro
🟩	San Antonio
🟪	San Francisco
🟪	San Jose
🟪	Santiago
🟪 🟦	São Paulo
🟦 🟧	Secaucus
🟪 🟦	Toronto
🟪 🟦	Washington Metro DC

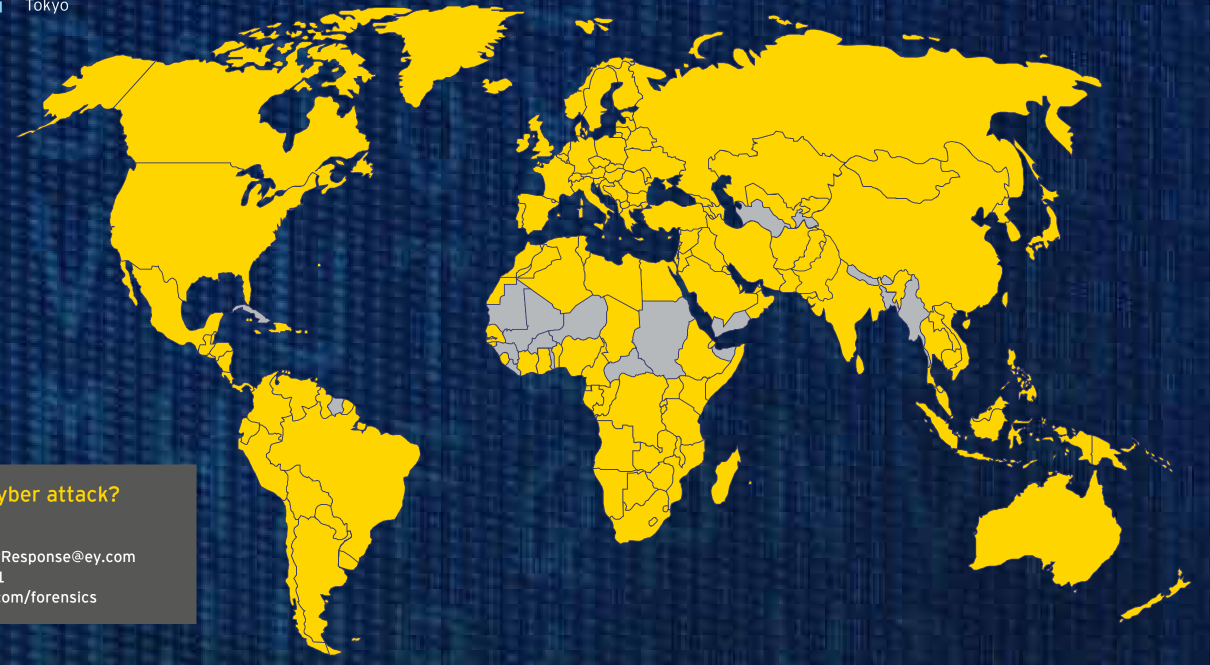
	Asia Pacific:
🟪	Adelaide
🟪	Auckland
🟪	Bangkok
🟪	Beijing
🟪	Brisbane
🟪	Hanoi
🟪 🟦	Hong Kong
🟪	Jakarta
🟪	Kuala Lumpur
🟪	Manila
🟪 🟩	Melbourne
🟪	Perth
🟪	Seoul
🟪 🟦	Shanghai
🟪 🟩 🟦	Singapore
🟪 🟦	Sydney
🟪	Taipei
🟪 🟦	Tokyo

	EMEA:
🟪 🟦	Amsterdam
🟪 🟩	Brussels
🟪	Bucharest
🟪	Budapest
🟧	Cologne
🟪	Copenhagen
🟪	Dublin
🟪	Düsseldorf
🟪 🟩 🟦 🟧	Frankfurt
🟪	Istanbul
🟪 🟦 🟧	London
🟪 🟩	Madrid
🟪	Manchester
🟪	Milan
🟪	Moscow
🟪 🟩	Oslo
🟪 🟩	Paris
🟪	Prague
🟪	Saarbrücken
🟪	Stockholm
🟪 🟦	Stuttgart
🟪	Vienna
🟪	Vilnius
🟪 🟩	Warsaw
🟪 🟦	Zürich

	Africa:
🟪	Abuja
🟪	Cape Town
🟪 🟦	Durban
🟪 🟦	Johannesburg
🟪	Nairobi

	Middle East:
🟪	Dubai
🟪 🟩	Tel Aviv

	India:
🟩	Chennai
🟪 🟦	Hyderabad
🟪 🟦 🟧	Mumbai
🟪 🟧	New Delhi



🟨	Countries with EY presence
🟪	Forensic labs
🟩	Advanced security centers
🟦	Forensic data centers
🟧	Managed Document Review centers

**Are you suspicious of a cyber attack?
Contact us now!**

Global incident intake email: CyberResponse@ey.com
Americas hotline: +1 855 611 8781
Contacts outside of Americas: ey.com/forensics

EY | Assurance | Tax | Transactions | Advisory

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

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

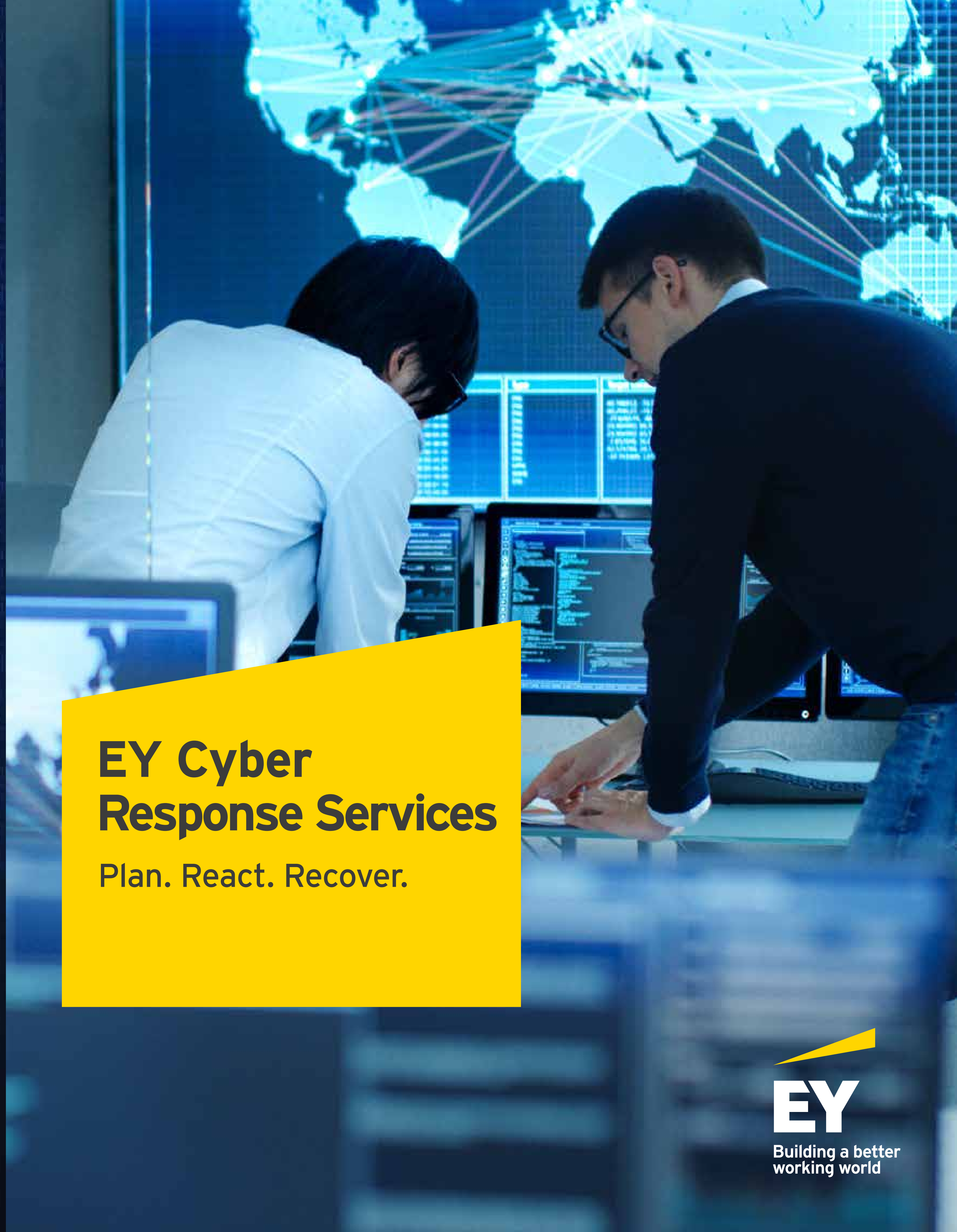
About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG no. 011340-18Gbl
BSC no. 1805-2686911

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

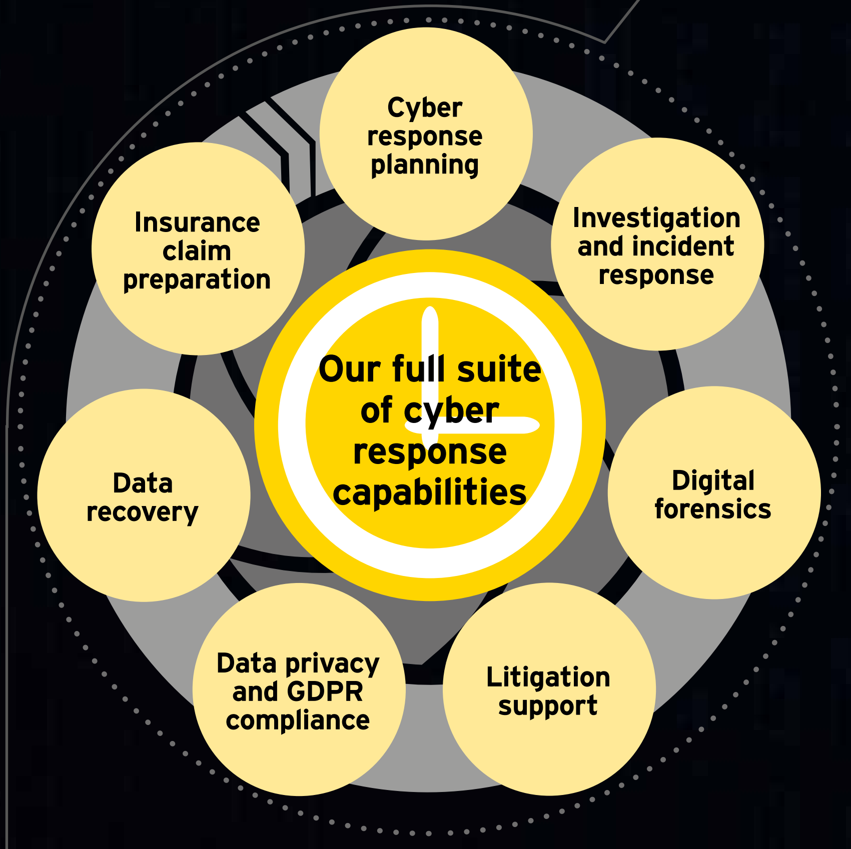


EY Cyber Response Services

Plan. React. Recover.

Building a better working world

How **EY** can help


Cyber response planning
Investigation and incident response
Digital forensics
Litigation support
Data privacy and GDPR compliance
Data recovery
Insurance claim preparation
Our full suite of cyber response capabilities

Cyber response planning

As part of their enterprise crisis management program, we help organizations develop plans and conduct simulation testing by taking into consideration of the magnitude and types of cybercrimes, data loss, customer privacy violation, regulatory compliance and infrastructure damage.

Our team helps organizations establish an investigation framework and the forensic procedures to support the investigation. Forensic readiness is important if an organization is to be able to quickly respond to an incident and conduct investigations with efficiency and accuracy. It also helps to safeguard evidence collection and preservation in compliance with relevant regulations or laws, and with minimal interruption to business operations.

We also work with organizations to form recovery plans that include containment and eradication, and leverage the broader business continuity plan. We take into account short-term measures to secure high-priority environments, restrict access or introduce barriers, while keeping our sights on a long-term mitigation strategy to reduce the risk of similar attacks happening again.

Investigation and incident response

Our cyber response team comprises investigators, formal regulators and law enforcement, as well as information security professionals who collaborate closely to pinpoint and contain the affected systems and data, conduct root cause analysis, perform eradication and mitigation activities, and liaise with government agencies as needed.

Our cyber investigators combine computer forensic knowledge with traditional investigative approaches, including interviewing witnesses, interrogating data, and examining physical and digital evidence to uncover the facts pertaining to a cyber incident. We work with organizations to customize the investigation approach for each incident, taking into account potential litigation and regulatory inquiries, resource requirements, timing, desired work product and budget.

As cybercrimes often span international borders with unique data privacy and state-secret laws, we tailor our procedures to the specific legal and regulatory requirements of each country involved in the investigation, including our work with counsel.

Digital forensics

Our global team is able to perform time-critical data mapping and forensically sound preservation and collection activities around the world simultaneously. In the event of an attack, we can quickly deploy resources around the world to collect investigative evidence, such as network traffic capture, log file and static host-system image. We analyze collected network log files and host information, and use internal cyber threat intelligence data, coupled with external threat intelligence data, to detect hostile activities and work toward attribution of the sources of the attack.

We also utilize forensic data analytics to collect and fuse data from multiple logging and audit-trail systems to piece together the attack timeline and discover the original point of entry, as well as subsequent attacker activities.

Litigation support

Almost all large cyber attacks lead to litigation, and, moreover, lead to different types of litigation handled by multiple law firms. We work with organizations and their counsel to develop work products consistent with litigation evidentiary requirements. Procedures for chain of custody, security of exhibits and contemporaneous note-taking practices are standard components of the methodology our professionals follow.

Many national security-related cyber investigations involve complex liaison with government authorities. EY's cyber response professionals are experienced in working with national security and law enforcement bodies, as well as management and counsel, to safeguard the organization's interests.

Data privacy and GDPR compliance

Data privacy is an important consideration of cyber response planning. We work with organizations to develop strategies and mechanisms to enable them to securely process and transfer the data needed for an investigation. Working with counsel, we develop written protocols that help them comply with applicable regulatory requirements.

Companies often need to achieve a basic level of understanding of the scope of the breach to determine the appropriate notification procedures, as required by regulations such as the GDPR. We help organizations conduct swift and concise investigations in order to understand the scope of the breach and to determine the appropriate notification procedures.

Data recovery

If cyber incidents result in destruction or corruption of data, EY can provide data recovery services and resources to support restoration from all types of deleted, corrupted, missing or inaccessible data that may have resulted from a cyber attack. This includes recovery of loss from any operating system environment and working with response teams to restore services.

Insurance claim preparation

We help organizations prepare and present a well-organized cyber claim with attendant supporting documentation. The goal during this part of the claim preparation process is to document and resolve as many components of the loss as possible. As organizations look to close out their cyber or network security claim, we help them to understand the calculations put forth by the adjusting team and develop alternative calculations for the resolution process.

Leader in Cybersecurity Consulting 2018

Source: ***The ALM Vanguard: Cybersecurity Consulting 2018***

24/7/365 rapid response

Through managed services or preferred provider arrangements, we forge long-term relationships with our clients that enables us to gain deep knowledge of their IT and data environments so we can offer the speed and confidence they need to respond to cyber attacks, regardless of the level of complexity.

With our global network, we have teams around the world who work together to forge a 24/7/365 incident intake process so we can respond to a cyber attack at any time of the day.

Secure global infrastructure and consistent global methodology

With numerous advanced security centers, forensic labs and data centers worldwide, all of which come with multiple layers of controls, we offer organizations the connectivity, scale and agility they need to respond to cyber attacks and to manage their data protection and privacy needs.

Governed by a globally consistent methodology, we offer integrated services from one stage of the response life cycle to the next, reducing the risks and costs of managing multiple service providers.

Multidisciplinary team

Our team includes cybersecurity professionals, investigators, data privacy professionals, digital forensics specialists, eDiscovery professionals, forensic accountants, government contract analysts, economists and certified fraud examiners, as well as former ethics and compliance officers, former government auditors, and former prosecutors and regulators.