Cyber breach response management

Breaches do happen.

Are you ready?

EY

Building a better
working world

Impacts

The impacts of cybercrime are growing in scale and complexity

The annual cost to the global economy from cybercrime is estimated to be US$445 billion.[1] As businesses across every industry fall victim to cyber attack, all corporate officers and functions – from the board, executive management, risk functions and general counsel to business units and information technology (IT) – are being profoundly affected.

Take, for example, a Fortune 50 global retailer that disclosed a data breach in September 2014. After stealing credentials from a vendor, hackers were able to break into the retailer's networks, install malware, and steal 56 million credit card numbers and 53 million email addresses over five months before the compromise was discovered and eradicated. This has had operational, legal and financial impacts. The retailer hired two external forensic investigation firms to investigate and remediate the technical aspects of the breach. In addition, five outside law firms were engaged in order to address the legal ramifications of over 40 civil suits stretching across multiple countries, in which customers and financial institutions have alleged negligence in protecting consumer data. The retailer is further being investigated by several state attorneys general in the United States. As the company's own SEC filing stated, "These claims and investigations may adversely affect how we operate our business, divert the attention of management from the operation of the business, and result in additional costs and fines."

Significant business impacts, however, do not result solely from the release of customer information. A multinational conglomerate became the victim of both data theft and destruction when attackers destroyed an undisclosed number of computers, and forced the company to shut down parts of its networks for periods ranging from days to months. From the terabytes of data that attackers claim to have stolen, they have already released emails and documents that contain embarrassing exchanges between company executives, sensitive business information and employees' personally identifiable information (PII). In addition to several class action lawsuits filed by employees who allege that the company did not take sufficient steps to protect their information, industry insiders believe that further lawsuits could emerge based upon the underlying data made public. Moreover, some of the sensitive business information disclosed could impact future contract negotiations with suppliers and partners, not only for the company in question, but also its entire industry.

These breaches demonstrate that it is the breadth of an attack's impact, separate and apart from an attack's sophistication, that must drive the depth of response.

>>The risk of large-scale cyber attacks continues to be considered above average on both dimensions of impact and likelihood. This reflects both the growing sophistication of cyber attacks and the rise of hyper connectivity … .<<

Global Risks Report 2015, World Economic Forum

[1] According to a report conducted by internet security company McAfee.

Response

Response to a breach must mature to address these wide-ranging business impacts

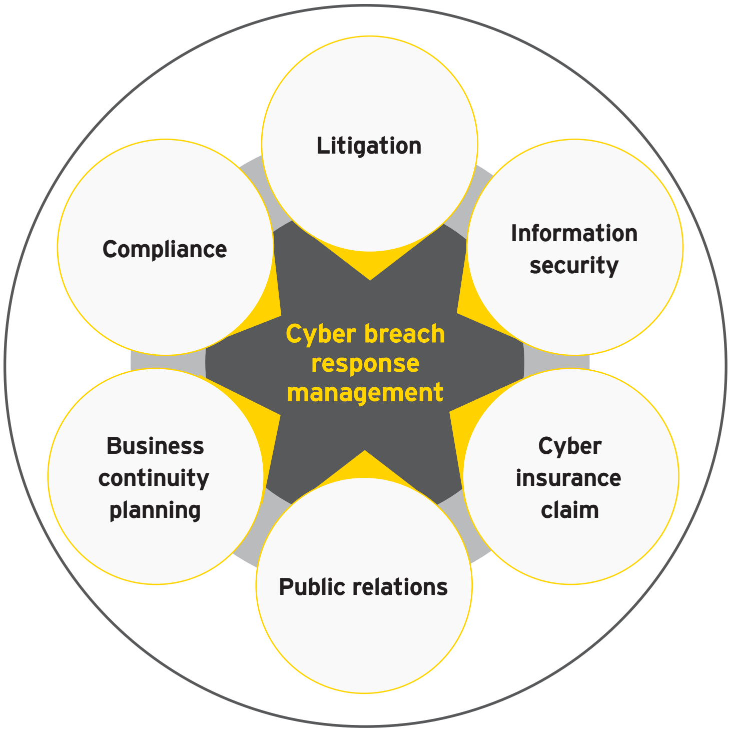
The potential impact of cybercrime requires that cybersecurity be viewed as a business risk, rather than a simple IT issue. Fundamentally, because a cyber attack may affect a business's operations, financial statements and legal exposure, its reputation is on the line. While businesses worldwide have increased the priority of cybersecurity risk, their focus has been primarily on protecting their information by preventing breaches; unfortunately, the current threat environment is such that it is only a matter of time before all businesses will suffer a major cyber breach. In order to adequately address these likely large and complex breaches, it is necessary for companies to develop a strong, centralized response framework as part of the enterprise risk management strategy.

A centralized, enterprise-wide cyber breach response program (CBRP) is the focal point that brings together the wide variety of stakeholders that must collaborate to resolve a breach. It needs to be run by someone who is equipped with in-depth legal, compliance and technology experience, and is able to manage the day-to-day operational and tactical response. The CBRP goes beyond the capacity of a traditional program management office (PMO). In its coordination and oversight role, the CBRP can help ensure that an organization's business continuity plan is appropriately implemented, develop and enforce a communication and briefing plan among all internal stakeholders, and centrally manage all breach-related inquiries received from external and internal groups. In short, it provides guidance to all lines of business involved in the response, sets a level of understanding about what information is critical for senior leaders to know — as well as when and how to express it, and allows continuous reaction with precision and speed as a breach continues to unfold over days, weeks or even months.

>>I am convinced there are only two types of companies: those that have been hacked and those that will be.<<

Robert Mueller, Former FBI Director

Figure 1: EY cyber breach response management framework



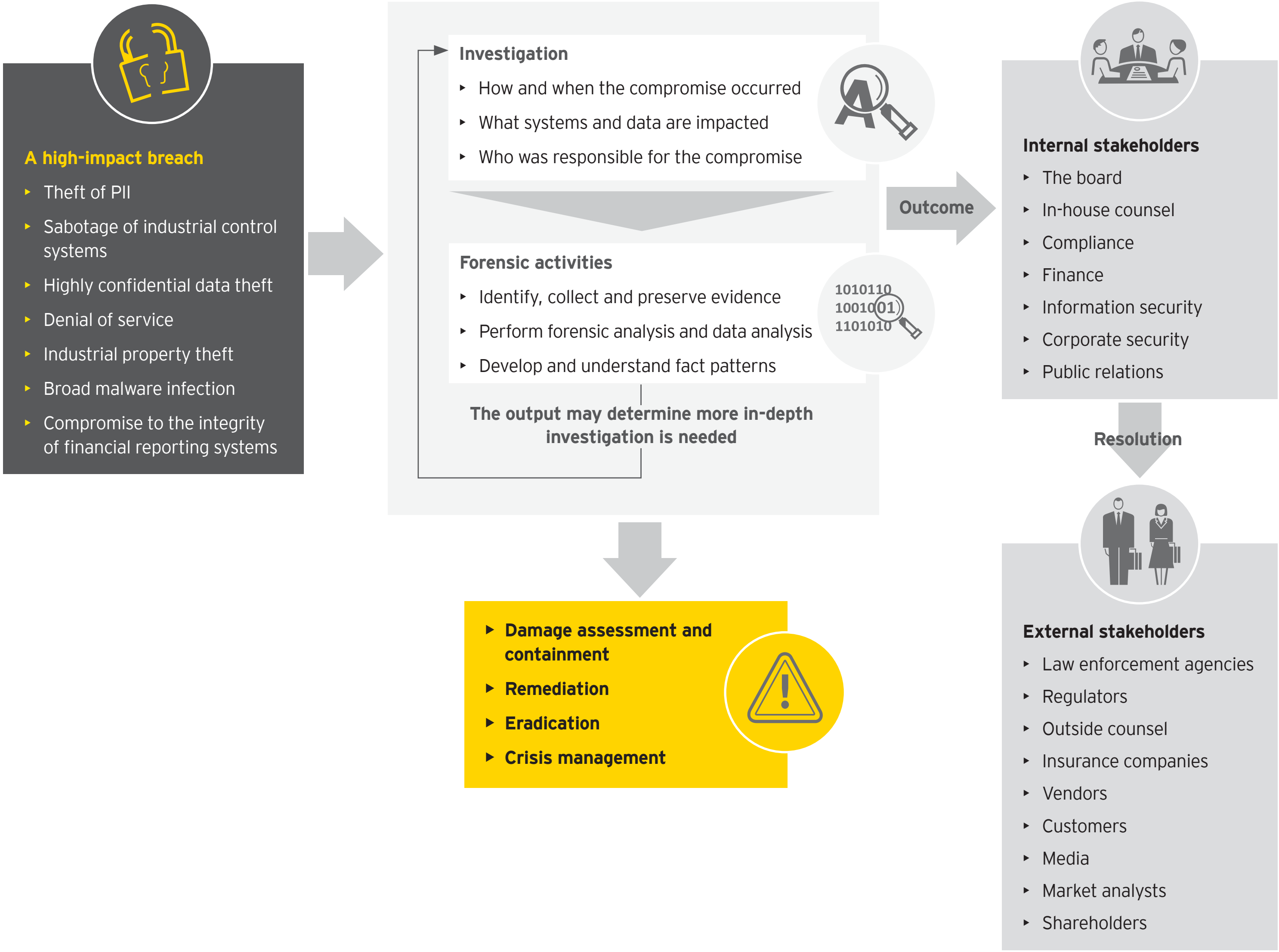
Key stakeholders

The roles of key stakeholders in a major cyber breach response

An effective CBRP must include the key constituencies in a high-impact breach. Even as investigators need to work closely with information security and IT personnel to determine the attack vector, exploited networks and systems, and the scope of assets stolen or impacted, a CBRP is the linchpin of the response. The CBRP not only oversees the process of evidence identification, collection and preservation, forensic data analysis, and impact assessment, but also can direct and modify the investigation based on fact-pattern analysis.

The CBRP helps ensure the smooth and timely flow of information among the internal stakeholders and helps the organization navigate the complexities of working with outside counsel, regulators and law enforcement agencies. The CBRP thus allows for a quick and cost-effective response that mitigates breach impacts by integrating the stakeholders and their knowledge, resulting in proficient cyber breach response management throughout the life cycle of a breach.

Figure 2: Who and what is involved in a high-impact cyber breach response?



A high-impact breach

- Theft of PII
- Sabotage of industrial control systems
- Highly confidential data theft
- Denial of service
- Industrial property theft
- Broad malware infection
- Compromise to the integrity of financial reporting systems

Investigation

- How and when the compromise occurred
- What systems and data are impacted
- Who was responsible for the compromise

Forensic activities

- Identify, collect and preserve evidence
- Perform forensic analysis and data analysis
- Develop and understand fact patterns

The output may determine more in-depth investigation is needed

- **Damage assessment and containment**
- **Remediation**
- **Eradication**
- **Crisis management**

Internal stakeholders

- The board
- In-house counsel
- Compliance
- Finance
- Information security
- Corporate security
- Public relations

External stakeholders

- Law enforcement agencies
- Regulators
- Outside counsel
- Insurance companies
- Vendors
- Customers
- Media
- Market analysts
- Shareholders

Risk oversight should be a function of the full board. The board must understand both the scope of the compromise and its existing and potential impact in order to guide the overall response strategy. The strategy would include communicating with employees, the public, shareholders and, mostly likely, regulators and law enforcement. The board should receive regular briefings from the CBRP leader with the latest investigative findings, regulator and law enforcement inquiries, litigation filings, media coverage and reactions of major shareholders. The board (or audit committee) also needs to work in lockstep with the chief financial officer (CFO) and the external auditor.

The CFO and the auditor have an intricate role in the cyber breach response. The auditor needs to verify the integrity of the company's financial controls and data, understand the potential adverse financial impact of the breach and evaluate the appropriate disclosures to be made in the financial reports, all of which have a direct impact on the board's communication strategy with the stakeholders and the broader public. While it is the board's and management's responsibilities to ensure that SEC disclosure requirements are met for breaches that rise to the level of materiality, auditors would be concerned with evaluating the sufficiency of such disclosure. Finallly, as large-scale breaches always have some financial impact, the CFO has a key role in filing insurance claims.

In-house counsel is integral to nearly all response activities. In large data breaches, it is almost certain that there will be regulator involvement and multiple litigation matters; in-house counsel, therefore, will need to communicate with regulators and collaborate with external counsel. If the breach involves intellectual property or critical infrastructure data that can be considered a national security breach, the in-house counsel must interact with the appropriate government and law enforcement agencies. In-house counsel needs to be equipped with as much information as possible about the scope of the breach in order to determine its potential compliance and legal impacts and interface effectively with various parties.

Another area of involvement for in-house counsel is collaboration with the information security team, public relations (PR), human resources (HR), vendors and external forensic investigators in practical matters such as evidence gathering, identification and discovery, as well as internal and external communication. In addition, in-house counsel will likely be working with the CFO on complications related to the cyber insurance claims.

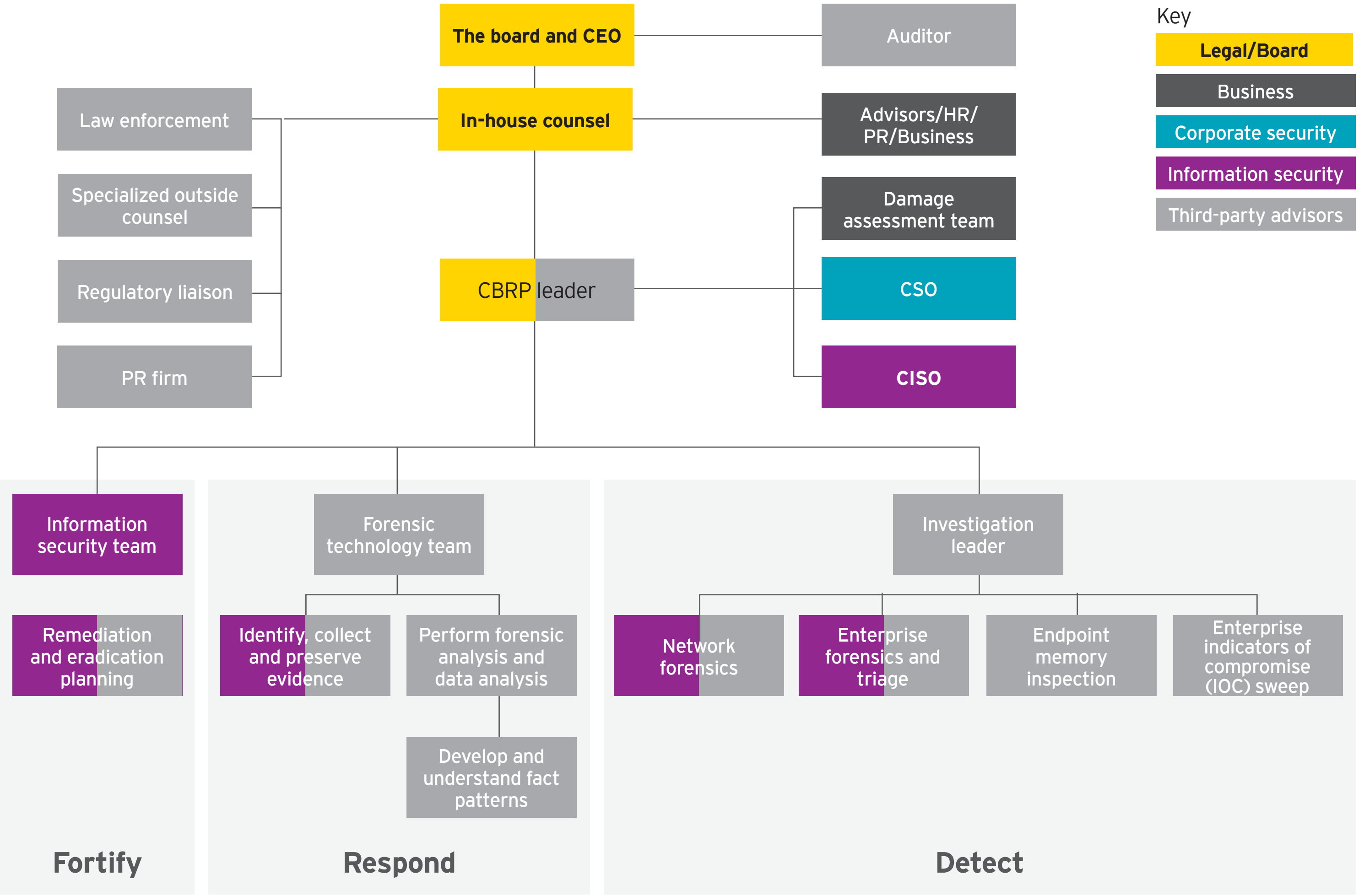
These functions require that in-house counsel be prepared to make countless decisions rapidly and accurately throughout the cyber breach response life cycle. The CBRP can greatly assist the response by taking away a significant portion of in-house counsel's time-consuming coordination burden by supplying more in-depth and accurate insights from multiple business units in a more timely fashion.

The Chief Compliance Officer (CCO) is internally responsible for the compliance program. In the event that a data breach involves PII, the CCO must ensure that all parties involved adhere to data privacy and disclosure laws. These laws can vary not only from country to country but also on a jurisdiction-by-jurisdiction basis. Because a major cyber breach can often involve people and information in several countries, a CCO can face challenges in addressing the disparity — and sometime even conflict — between countries' regulations. The CCO must work closely with in-house counsel, the board and the executive team as it manages compliance risks.

In more mature organizations, a corporate security officer (CSO) may exist whose role includes responsibility for the overall security of the corporation. The CSO protects all assets — whether physical, IT, intellectual property or people — against all threats — whether from opportunistic crime, foreign espionage, sabotage or protest groups. The CSO generally interacts with national security authorities and law enforcement, as well as other organizations in similar industry sectors. In regulated industries, government and defense contracting, and critical national infrastructure services, the CSO is often accountable for compliance with national legislation governing security as part of the organization's "license to operate."

The chief information security officer (CISO) and the information security team are at the heart of the operational response. Working with the investigation team, they must quickly determine the root cause of the attack and define the scope of the breach — data stolen, systems impacted and level of penetration — in order to develop and execute a plan for eradicating the threat and performing any remediation activities. The CISO usually has the closest interaction with the investigators, working with the CBRP leader and IT personnel. It is also the CISO's responsibility to ensure that relevant investigative information is quickly funneled to the response team. The initial investigative findings are critical for evidence gathering and forensic analysis, which, in turn, will allow for the production of impact assessments and various data and reports required for other response activities, such as litigation and regulatory reporting. By the same token, the CISO needs to stay abreast of all response activities and ensure that the final output of the enterprise-wide response is carefully studied and that lessons learned are used to strengthen the company's information security strategy and future responses.

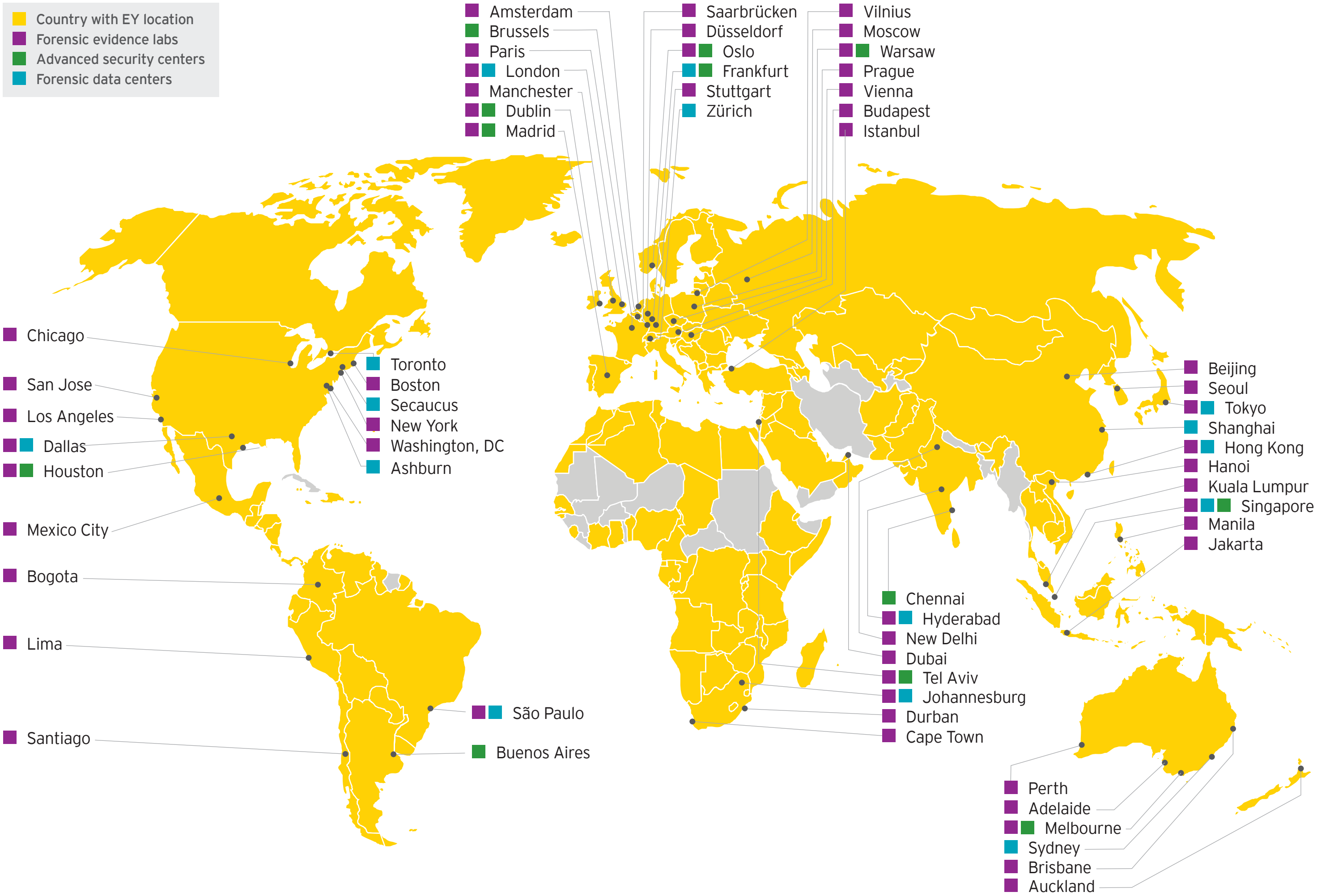
Figure 3: A sample organization structure in response to a large-scale cyber breach


The board and CEO
Auditor
Key
Legal/Board
Business
Corporate security
Information security
Third-party advisors
Law enforcement
In-house counsel
Advisors/HR/ PR/Business
Specialized outside counsel
Damage assessment team
Regulatory liaison
CBRP leader
CSO
PR firm
CISO
Information security team
Forensic technology team
Investigation leader
Remediation and eradication planning
Identify, collect and preserve evidence
Perform forensic analysis and data analysis
Network forensics
Enterprise forensics and triage
Endpoint memory inspection
Enterprise indicators of compromise (IOC) sweep
Develop and understand fact patterns
Fortify
Respond
Detect

How EY can assist you

From forensic investigation to litigation, to working with regulators, law enforcement, and national security and intelligence agencies, our team has the scale, experience and credibility you need to respond to and recover from a cyber breach in a comprehensive manner. Our team includes cybersecurity professionals, investigators, 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. We have more than 60 forensic technology centers worldwide, and we can provide resource-based services through our network in all countries where EY has offices.

Figure 4: The global presence of our cyber breach response teams



Cyber breach response management

Impact assessment

Utilizing advanced data analytics tools, EY can help you understand the content of the data that has been stolen in order to identify the impact of the breach. We can also help to develop proactive damage control plans that are comprehensive in considering the magnitude and types of data stolen, as well as targeted to particularly sensitive information.

Litigation support

Almost all large cyber breaches lead to litigation, and, moreover, lead to different types of litigation handled by multiple law firms. As forensic technology and accounting professionals, we work with our clients and their outside counsel to tailor our work product and procedures for use as evidence in legal proceedings. Procedures for chain of custody, security of exhibits and contemporaneous note-taking practices are included within a broader set of quality and risk management procedures that our professionals follow.

Many national security-related cyber investigations involve complex liaison with government authorities, who may favor allowing a corporate cyber attack to continue for investigative purposes. EY's cyber investigation professionals are skilled in working with national security and law enforcement bodies, as well as management and counsel, to safeguard the organization's interests.

Support for parallel proceedings

Managing a cyber breach response requires several streams of work — from regulatory filings, to litigation response, to public communication — to be carried out simultaneously. This necessitates everything from technical to regulatory expertise. Our experience with large, multinational firms responding to cross-cutting issues has allowed us to develop the knowledge and relationships that transfer seamlessly to help our clients navigate their response to a major cyber breach.

End-to-end eDiscovery engagement support

While major cyber breaches usually lead to multiple litigation matters, we are able to look for commonalities across all cases, allowing us to develop an optimal eDiscovery process that is responsive to all legal matters. We offer seamless integration from one stage of the eDiscovery life cycle to the next, reducing the risks and costs associated with managing multiple service providers. Further, our team can help project teams and counsel understand the impact of loss when the stolen documents and information can be identified.

Discovery Advisory and PMO Services

Our eDiscovery professionals are experienced discovery project managers, accustomed to working closely with companies and outside counsel to help manage high-pressure engagements; they are well-equipped to manage a Discovery project resulting from a cyber incident. We view the development of an effective communication plan, supported with key summary and progress reports, as critical components in our ability to provide clients with valuable insight into each engagement phase.

Cyber investigation

Cybercrime diagnostic

We help companies proactively detect attacks using forensically sound techniques to protect the integrity of evidence and investigation. Our diagnostic services typically include log data analysis, live network log data analysis, live network traffic analysis and host-based forensic analysis.

Fact finding, live interviews and evidence collection

Our cyber investigative resources combine computer forensic expertise with traditional investigative approaches, including interviewing witnesses, interrogating data, and examining physical and digital evidence to uncover all facts pertaining to a breach. We can determine what data was compromised and whether digital evidence was potentially deleted or modified, recover data and recreate events. These results can then be used to refine and further develop other aspects of the cyber response plan.

Investigative planning and scope setting

A complex cyber breach requires extensive investigation to support technical recovery and remediation, as well as all associated legal actions. We work with our clients to co-develop a customized investigation approach for each legal matter, including specific areas of inquiry and potential procedures, experienced resources, timing, work product and budget. As cyber breaches 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.

Cyber forensics

Identification, preservation and collection

Whether we conduct the initial investigation or not, we work with the first line of investigation team to identify evidence based on its findings. Our team will perform time-critical electronically stored information (ESI) mapping and forensically sound preservation and collection activities domestically, globally and simultaneously.

Our cyber forensic collection teams can be quickly deployed to collect three main sources of investigative evidence:

- Network traffic capture: We can record full network traffic from multiple network trunks for months at a time to allow "forward and backward" analysis of cyber attacks in progress.
- Log file collection: We can capture and store months of log files from firewall, proxy, webserver, mail gateway, server, application and transaction logs.
- Static host system image collection: We can use either active tools or passive collection techniques to collect evidence artifacts from laptop, desktop and server computer systems that show evidence of attacker behavior – including copies of zero-day malware or "dropped" attack tools, such as remote access Trojans (RAT) and other hidden remote access, privilege escalation and data exfiltration tools.

Transaction analysis and anomaly assessment

Using state-of-the-art automated tools, the EY forensics team can rapidly deploy and execute transaction analysis and anomaly detection to distill investigative data to the most critical data points. Large volumes of data can be analyzed rapidly and structured/unstructured data from disparate systems can be integrated to advance investigations and contain breaches. Relevant information is cross-referenced to various systems, significantly reducing the time of the investigative life cycle.

Computer forensics and compromise analysis

Our cyber forensics teams analyze collected network log files and host information and use internal cyber threat intelligence data, coupled with external threat intelligence data on IOC, to detect hostile activity and work toward attribution of the sources of the attack.

Large-scale cyber threat data analytics

We utilize our considerable forensic data analytics systems to collect and fuse data from multiple cybersecurity logging and audit trail systems to piece together the attack timeline and discover the original point of entry, as well as subsequent attacker activities. This often involves collection and fusion of terabytes of firewall, proxy, webserver, mail gateway, server, and application and transaction logs for investigative analysis.

Data recovery and remediation

Data recovery

If cyber breaches 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.

Remediation planning

EY works with companies to form response teams and establish a containment and eradication strategy, often incorporating short-term measures that secure specific environments, restrict access or introduce barriers. An important component of a remediation planning exercise also involves strengthening an organization's security posture following any system breach. We utilize leads and inputs developed with a variety of assessment tools to identify enhancements to systems, while mitigating critical vulnerabilities.

Unstructured and structured data processing and hosting

Investigative data sets are typically so large and complex that it is difficult to process with in-house data management tools or traditional data processing capabilities. EY has advanced platforms and knowledge to securely host large volumes of client data for any number of investigative tasks. We work with our clients to extract, transfer and host data from multiple sources, including high bandwidth voice, text and video streams.

Managed document review

We provide law firms and corporate legal departments that are involved in cyber breach-related litigations with secure and scalable review facilities that are fully integrated with EY's proprietary technology platform.

Information governance

We help organizations implement a well-balanced information governance program that aligns with their risk management strategy, and that can be effectively operationalized to protect information assets and accomplish broader business goals.

Data privacy advisory

We work with our clients to develop strategies and mechanisms to enable ESI to be securely processed and transferred to the jurisdiction in which production is required in compliance with applicable requirements and complete with standardized written protocols.

Cyber and network security insurance claims

Preliminary loss estimate

EY assists in identifying all potential loss components, developing a strategy to efficiently quantify those elements, and preparing a preliminary estimate of the loss so that you can share information quickly with your insurers and obtain a cash advance. We consult with your team regarding potential loss categories to assemble the claim calculation in accordance with insurance policy requirements. EY's combination of forensic accountants and technology professionals assist our clients to identify what happened technologically, determine how that fits into the company's policies, and accelerate the time frame of the claims process and, ultimately, the timeliness of cash recoveries.

Claim development and submission

We help our clients to 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.

Claim resolution

As you look to close out your cyber or network security claim, we help you to understand the calculations put forth by the adjusting team and develop alternative calculations for the resolution process.

Know what you don't know

One of the biggest dangers in a cyber breach response is that a company will not know the full extent of the damage immediately after a cyber attack. Stolen information may not be made public all at once or utilized immediately — criminals must first review the data that they have obtained and determine how best to use it.

Companies are at a distinct disadvantage if they learn about their stolen information from the media. They need to be proactive to get ahead of the criminals. By combining advanced data analytics tools and firsthand knowledge of the organization, companies can understand what exists within the stolen data — whose emails, what documents, which topics — so that they know what may become public and develop forward-leaning response plans should it become so. We are able to determine what may have been stolen by a variety of methods, including:

- Analysis of forensic artifacts or log data that reveals which information or systems the attackers accessed or removed
- Detection of IOC on systems containing information that might have been stolen
- Detection of actual packages of information prepared for exfiltration by the attacker
- Detection of actual exfiltration in progress across network connections
- Recovery and analysis of backup data from systems that were attacked and damaged

Below are some advanced forensic data analytics tools that can help companies analyze stolen data, gain insight into the potential impact and work to mitigate any negative outcomes.

Social network analysis

Social network analysis tools can reveal and map the full scope of an employee's communication. When applied to stolen data, this can help companies quickly get a handle on the breadth of interactions and exchanges employees in senior or sensitive positions may have had.

Topic extraction

Just as social network analysis tools can define the interaction of key players present in a stolen tranche of data, topic extraction can similarly scope the range of issues discussed. Topic extraction tools are able to classify the broad themes present in a given dataset, which enables the investigative team and company to quickly get an understanding of what information — and how sensitive it might be — has been stolen.

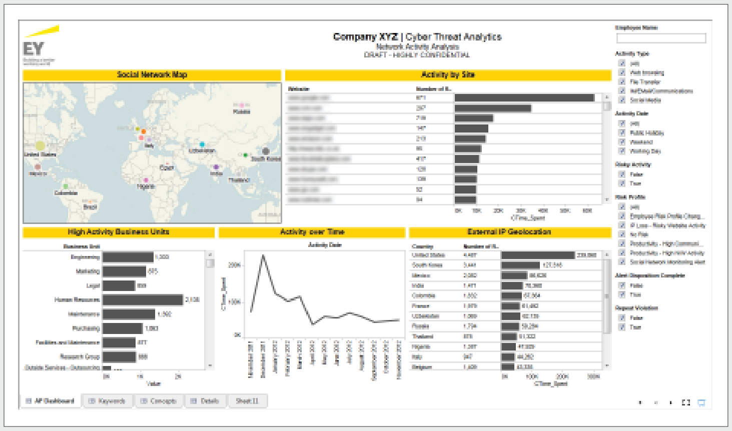
Linguistic analysis

Linguistic analysis tools allow companies to home in on data — both structured and unstructured — that may be sensitive in some manner. When emotive tone analysis captures different emotions across a communication chain, a company can gain insight into communication that may be of concern. Going beyond emotive tone identification, ethical red flag analysis can identify documents and communication that may be evidence of insider threat and rogue employee behavior.

Document clustering and predictive classification

Document clustering technologies group documents by a number of different features, such as by metadata (e.g., file names and dates) or by the content of the documents themselves. Additionally, unstructured data can be classified through advanced machine-learning systems and methodologies. This predictive classification can be used to separate out documents of interest.

Figure 5: Sample comprehensive alert monitoring dashboard combining multiple data analytics results



Company XYZ | Cyber Threat Analytics
Network Activity Analysis
DRAFT - HIGHLY CONFIDENTIAL

Contacts

To find out more about how our Fraud Investigation & Dispute Services (FIDS) services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/FIDS.

Global and Americas

David Remnitz
Global and Americas FIDS Forensic Technology & Discovery Services (FTDS) Leader
+1 212 773 1311
david.remnitz@ey.com

Area FIDS FTDS Leaders

EMEIA

Paul Walker
+44 20 7951 6935
pwalker@uk.ey.com

Asia-Pacific

Reuben Khoo
+65 6309 8099
reuben.khoo@sg.ey.com

Japan

Hiroyuki Kaiyama
+81 3 3503 1100
kaiyama-hryk@shinnihon.or.jp

Relevant thought leadership

Overcoming compliance fatigue
Reinforcing the commitment to ethical growth
13th Global Fraud Survey
EY
Building a better working world

Overcoming compliance fatigue Reinforcing the commitment to ethical growth

13th Global Fraud Survey

Get ahead of cybercrime

Global Information Security Survey 2014

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 organizations 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's Fraud Investigation & Dispute 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 industry sector. With our more than 3,200 fraud investigation and dispute professionals around the world, we assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. And 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. WW0385
1503-1420071
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