Sponsored by: EY Forensic & Integrity Services

Legal, Compliance and Technology Executive Series

Who and what is involved in a high-impact cyber response?

Responding to a complex cyber incident requires extensive investigation to support recovery, remediation, regulatory inquiries, litigation and other associated activities. Organizations need to conduct competent investigations with speed and precision. Otherwise, the financial and reputational impact can be profound - including, but not limited to: risk revenue loss from disruption to the business, regulatory fines from noncompliance and loss of customer trust.

This paper intends to provide a foundational understanding of the stakeholders and key activities involved in responding to a major cyber attack.

Of special interest to:

Legal counsel
Corporate security officers
Information security executives
Compliance executives
Risk management executives
Internal audit

EY
Building a better working world

Who is involved?

In the event of a large, complex cyber attack, there are many stakeholders who will be affected. Their involvement in response activities is critical. However, effective and timely response requires more than just their involvement — close and around-the-clock collaboration is key. Only when the stakeholders effectively work together can a timely, accurate and cost-efficient response be possible.

It is very common that an organization engages an independent third party to help manage the response activities in the event of a major cyber attack. The third party needs to possess in-depth legal, compliance and investigative experience in order to be able to effectively communicate with all stakeholders. Their role goes beyond the capacity of a traditional program management office. They help conduct timely and thorough investigations, activate the business continuity plan with precision, enforce a communication process among all stakeholders, and centrally manage all inquiries received from external and internal groups, as the incident continues to unfold over days, weeks or even months.

A high-impact incident

- Theft of personally identifiable information
- 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

First respondents

Investigative team

- Investigators
- IT forensics professionals
- Law enforcement

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 work product may determine more in-depth investigation is needed.

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

Outcome

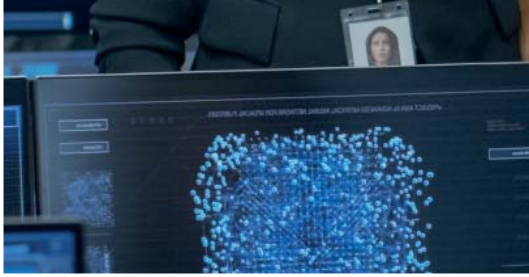
Internal stakeholders

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

Resolution

External stakeholders

- Law enforcement
- Regulators
- Outside counsel
- Auditors
- Vendors
- Customers
- Media
- Market analysts
- Shareholders



Addressing cyber breaches is a team sport – everyone should be involved

Board

Risk oversight is a function of the full board. The board oversees the response strategy that includes communicating with employees, the public, shareholders and, mostly likely, regulators and law enforcement. The board (or audit committee) also needs to work in lockstep with the CFO and the external auditor.

CFO

The chief financial officer (CFO) and the auditor have the responsibility to verify the integrity of the company's financial controls and data, understand the potential adverse financial impact of the incident and determine the appropriate financial disclosures in relevant filings, all of which have a direct impact on the board's communication with shareholders and the broader public.

In-house counsel

The in-house counsel has an active role in working with the forensic investigators in practical matters such as evidence gathering, root-cause analysis and electronic discovery. In-house counsel usually takes the lead in communicating with regulators and external counsel. They must quickly determine the incident's potential compliance and legal impacts to be able to interface effectively with various external stakeholders.

Communications

Internal and external communication teams are important to ensure that the incident is properly communicated to employees, customers, shareholders and other third parties who may be impacted. If properly educated, employees can be very helpful to facilitate the investigation and take necessary measures to stop the breach from spreading further. Timely communication to the public is critical to restore trust and to instill confidence in the organization's ability to manage cyber risk and minimize the incident's negative impact on its operations and customers.

Compliance and Ethics

The chief compliance and ethics officer is usually involved in the involved in cyber response as they are is responsible for assessing the regulatory compliance risk in the event of a cyber attack, whether it is related to data protection and privacy, or sector-specific regulations. A major cyber attack often spans multiple countries or jurisdictions; the CCO can face challenges in addressing the disparity — and sometimes even conflict — between juridictions. The CCO must work closely with privacy experts, the legal department, the board and the executive team as they manage these issues.

CSO

Many large organizations employ a corporate security officer (CSO), whose key responsibility is the overall security of all assets — whether physical, IT, intellectual property or people — against all threats, such as from accidental negligence, malignant insiders, professional criminals or state-sponsored groups. 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."

CISO

The chief information security officer (CISO) works closely with the investigation team to quickly determine the root cause of the attack, understand its scope and assess its risk impact — data stolen, systems impacted and level of penetration — in order to contain and eradicate the threat and perform remediation activities. The CISO should also carefully study the investigation results and gather helpful information so that lessons learned are used to strengthen the company's information security strategy and future responses.

In summary

A poor response may be worse than the actual cybercrime itself. A centralized cyber response plan is critical to bring together stakeholders who may have different priorities but must collaborate to resolve the cyber attack. A well-defined cyber response plan provides guidance to all lines of business involved in the response, sets a level of understanding about what information is critical in an incident — as well as when and how to express it — and allows continuous reaction with precision and speed as the event continues to unfold over days, weeks or even months.

What is involved?

The current threat environment is such that it is only a matter of time before an organization will suffer a major cyber attack. Organizations need to have a clear understanding of the key steps of cyber response in order to be adequately prepared when the crisis strikes. The five steps of cyber response have interdependencies on each other and they do not have to necessarily take place in sequential order. Performing the steps in parallel can shorten the time to resolution and reduce risk exposure.

1

Planning

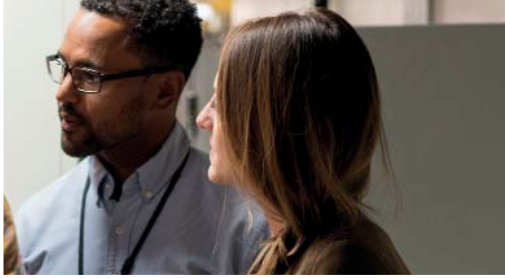
A cyber attack can go undetected for a long period of time. Consistently performing enterprise-wide monitoring and diagnostics is the key to early detection and resolution.

2

Identification and escalation

In this stage, knowledge of the enterprise network environment is critical as the response team isolates the incident and zeroes in on the affected systems and data. Depending on the severity, complexity and urgency of the incident, appropriate escalation procedures are enacted based on pre-established criteria. The triage guidelines should be continuously fine-tuned to stay current with the organization's risk environment so that critical risks are not missed and low-level risks don't take up precious resources.





Triage examples	
High-impact incidents	**Sample activities**
▸ Leakage of customer personally identifiable information ▸ Damage to physical infrastructure and control systems ▸ Intellectual property theft ▸ Enterprise-wide malware infection ▸ System-wide service attack	▸ Immediately engage the board, legal, compliance and PR ▸ Determine initial disclosures to external auditor, regulators, customers and third-party partners ▸ Activate business continuity plan
Medium-impact incidents	**Sample activities**
▸ Unauthorized remote access ▸ Unauthorized data transmittal ▸ Demilitarized zone exposure, weak credentials	▸ Conduct routine investigation to assess impact ▸ If the investigation results indicate potential high-impact risk, escalate the risk level immediately ▸ Otherwise, lower the risk level and handle accordingly
Low-impact incidents	**Sample activities**
▸ Misuse of computer equipment ▸ Illicit use of cloud file shares/removable storage ▸ Software piracy ▸ Access to illicit websites	▸ Conduct routine internal investigation

The five steps of cyber response

3 Investigation

Investigators usually work closely with information security to determine how and when the compromise occurred, the root cause and the impact to the organization. A major incident can involve several cycles of investigation and each cycle includes four key activities: evidence gathering, analysis, containment and eradication.

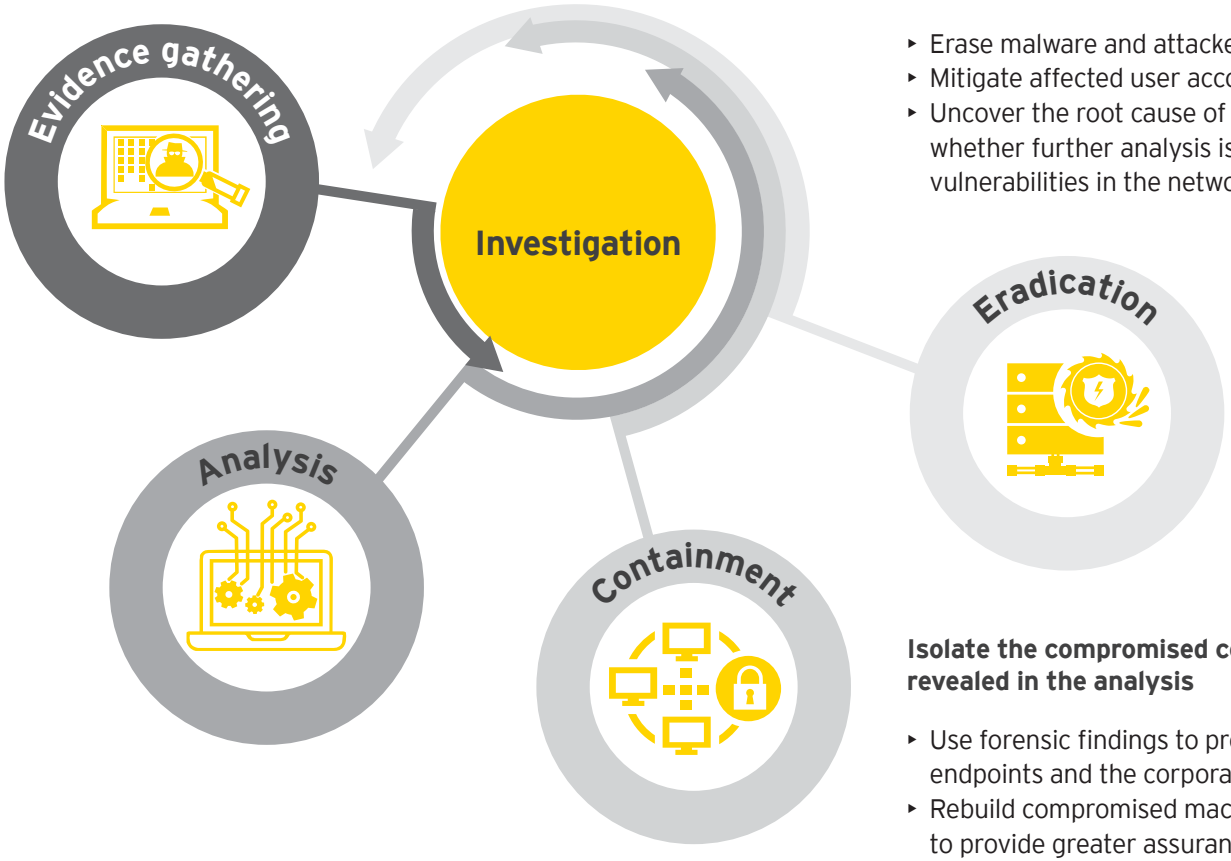
Evidence gathering needs to be conducted in a forensically sound manner so findings can stand up to legal and regulatory scrutiny. Analysis helps identify the root cause and contaminated computers and systems that should be isolated and removed so the virus doesn't spread further in the network. All three activities must be well coordinated and executed with speed and precision, as attackers will often try to re-establish a presence and entrench themselves into the network. Containment and eradication could reveal new risks that need to be analyzed further - the cycle of activities will continue until the system is back to its normal state and all exposed areas have been thoroughly studied and mitigated.

Identify, collect and preserve evidence

- Acquire all host-based evidence pertinent to the type of incident in a timely, efficient and forensically sound way
- Identify any running processes, open ports and remote users
- Collect network-based log files, including, but not limited to, routers, firewalls, servers and intrusion detection system (IDS) sensors
- Conduct necessary internal and external interviews

Perform forensic analysis and develop fact patterns

- Conduct a comprehensive forensic examination to determine the attack vector, the scope and depth of the compromise
- Identify any unauthorized user accounts or groups, rogue processes and services, and any unauthorized access points
- Tell the story of who, what, when, where and how



Remove key components of the security incident

- Erase malware and attacker tools
- Mitigate affected user accounts
- Uncover the root cause of the breach to determine whether further analysis is required to reveal other vulnerabilities in the network

Isolate the compromised computers and systems revealed in the analysis

- Use forensic findings to protect and secure endpoints and the corporate perimeter
- Rebuild compromised machines when necessary to provide greater assurance

The five steps of cyber response

4 Remediation

The compromised organization should identify and address vulnerabilities in the environment, sufficiently strengthen the environment to complicate the attacker's effort to get back in, enhance its ability to detect and respond to future attacks, and prepare for eradication events.

5 Resolution and lessons learned

This stage largely entails data preparation for the purpose of regulatory reporting, insurance claim, litigation, threat intelligence and/or customer notification. Beyond reactive activities, it's also important for the organization to turn a reactive crisis management case into lessons for proactive cyber risk management. The cyber response team should summarize information security improvement measures based on the investigation's outcome.

In summary

Cyber response consists of a series of stages that must be carefully planned. The plan needs to involve professionals with diverse backgrounds in investigation, information security, legal, regulatory compliance and communication. The response team needs to be able to mobilize at a moment's notice and work as a well-oiled machine. In order to do so, they should conduct tabletop exercises on a regular basis to make sure that skill sets are kept up-to-date with the latest threats, and communication links remain operational.

For more information, contact EY Cyber Response Services at:

CyberResponse@ey.com or visit us at: **ey.com/cybersecurity**

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. 011814-18Gbl
BSC no. 1805-2686911

ED None

ey.com