Cyber attacks do happen. Are you ready?

Why EY?

What makes EY well-positioned to help you?

- Globally integrated forensic investigative methodology and advanced cyber investigative capabilities
- End-to-end services deployed within a mature forensic investigative framework
- Advanced cyber analytics capabilities on big data platforms
- Dedicated industry teams
- Deep experience working with lawyers, regulators and law enforcement
- Global operational capabilities
- Investigations conducted in local languages using local resources
- Global methodologies and standard computer forensic certification process
- Defensible data standards acceptable to various global and local regulatory entities during investigations and disputes

The global presence of our cyber response team

“There are two kinds of companies. Those that have been hacked, and those that have been hacked but don’t know it yet.”

— Mike Rogers
House Intelligence Committee Chairman
### How to respond to cybercrime

In the event of a cyber attack, every organization should be sufficiently prepared to assess, investigate, remediate, eradicate and respond to regulatory and other disclosure requirements.

#### Preparation

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.

#### Triage

Isolate the incident and zero in on the impact. Knowledge of the enterprise network environment is critical. Based on the severity, complexity and urgency of the incident, determine whether the appropriate response includes a full-scope investigation following the cybercrime response plan.

#### Investigation

**Determine how and when the compromise occurred, what was the root cause and what was the impact to the organization. The investigation needs to be initiated and conducted with a great sense of urgency and in a secured environment. To do so, each organization should have a pre-established, scalable cybercrime response team consisting of relevant lines of business and executive functions, with defined roles and responsibilities, as well as internal and external communication protocols.**

**The effectiveness of the plan needs to be tested through tabletop exercises.**

**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.

**Develop and understand fact patterns**

Determine who is involved. Tell the story of who, what, when, where and how. Consider necessary disclosures as facts develop.

**Remediation**

Identify and address vulnerabilities in the environment, sufficiently harden the environment to complicate the attacker’s effort to get back in, enhance the ability to detect and respond to future attacks, and prepare for eradication events. This usually runs concurrently with the investigation.

Response to the root case of initial incident will likely start out as tactical but should further grow to be strategic. Companies should perform attack and penetration exercises to determine if tactical fixes were effective. Remediation usually runs concurrently with the investigation.

#### Eradication

Effective eradication plans must be well-coordinated and executed with speed and precision as the attackers will often try to re-establish a presence and entrench themselves into the network. Preparation for an eradication event starts during the investigation phase so that the eradication can start soon after the investigation is completed.

#### Outcome/resolution

Prepare data based on varying requirements for regulatory reporting, insurance claim and dispute, litigation, threat intelligence and/or customer notification. Cross-border collaboration is critical.

**Information governance**

Perform forensic analysis and data analytics

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.

**Prepare report of recommendations on disclosures, program improvement, discipline and remediation.**

**Identify potential initial disclosures to external auditor, regulators, customers and third-party partners**

**Immediatly initiate the cybercrime response plan**

**Conduct routine IT assessment to determine root cause**

If found immediately, take remediation measures

If not, conduct further investigation or continue to monitor, pending further action

**Draw conclusions and make recommendations**

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.

**Identify and address vulnerabilities in the environment, sufficiently harden the environment to complicate the attacker’s effort to get back in, enhance the ability to detect and respond to future attacks, and prepare for eradication events.**

**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.

**Develop and understand fact patterns**

Determine who is involved. Tell the story of who, what, when, where and how. Consider necessary disclosures as facts develop.

**Remediation**

Identify and address vulnerabilities in the environment, sufficiently harden the environment to complicate the attacker’s effort to get back in, enhance the ability to detect and respond to future attacks, and prepare for eradication events. This usually runs concurrently with the investigation.

Response to the root case of initial incident will likely start out as tactical but should further grow to be strategic. Companies should perform attack and penetration exercises to determine if tactical fixes were effective. Remediation usually runs concurrently with the investigation.

#### Eradication

Effective eradication plans must be well-coordinated and executed with speed and precision as the attackers will often try to re-establish a presence and entrench themselves into the network. Preparation for an eradication event starts during the investigation phase so that the eradication can start soon after the investigation is completed.

#### Outcome/resolution

Prepare data based on varying requirements for regulatory reporting, insurance claim and dispute, litigation, threat intelligence and/or customer notification. Cross-border collaboration is critical.

**Information governance**

Perform forensic analysis and data analytics

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.

**Prepare report of recommendations on disclosures, program improvement, discipline and remediation.**

**Identify potential initial disclosures to external auditor, regulators, customers and third-party partners**

**Immediatly initiate the cybercrime response plan**

**Conduct routine IT assessment to determine root cause**

If found immediately, take remediation measures

If not, conduct further investigation or continue to monitor, pending further action

**Draw conclusions and make recommendations**

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.

How can EY help?

Our end-to-end information security and cybercrime services provide proactive and reactive assistance to help our clients manage cyber risks.

- Legal and regulatory response
  - Impact assessment
  - Litigation support
  - Support for parallel proceedings
  - End-to-end eDiscovery engagement support
  - Discovery advisory and PMO services

- Cyber investigation
  - Fact finding, live interviews and evidence collection
  - Investigative planning and scope setting
  - Identification, preservation and collection
  - Transaction analysis and anomaly assessment
  - Computer forensics and compromise analysis
  - Host, network, cloud and malware analysis

- Data recovery and remediation
  - Data recovery
  - Remediation planning
  - Unstructured and structured data processing and hosting
  - Managed document review
  - Information governance
  - Data privacy advisory

- Cyber and network security
  - Insurance claims
  - Preliminary loss estimate
  - Claim development and submission
  - Claim resolution

- Information governance
  - Program improvement recommendations and follow-up

**To conduct a cyber investigation of a targeted attack, a company requires four critical capabilities:**

- Network forensics and network visibility
- Enterprise memory forensics
- Enterprise host-based forensics
- Enterprise sweep

Contact us at: cyberresponse@ey.com