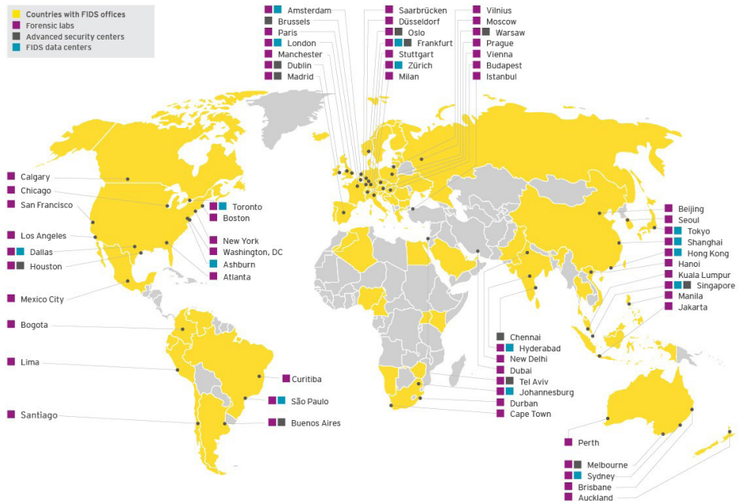
Why EY?

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

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.

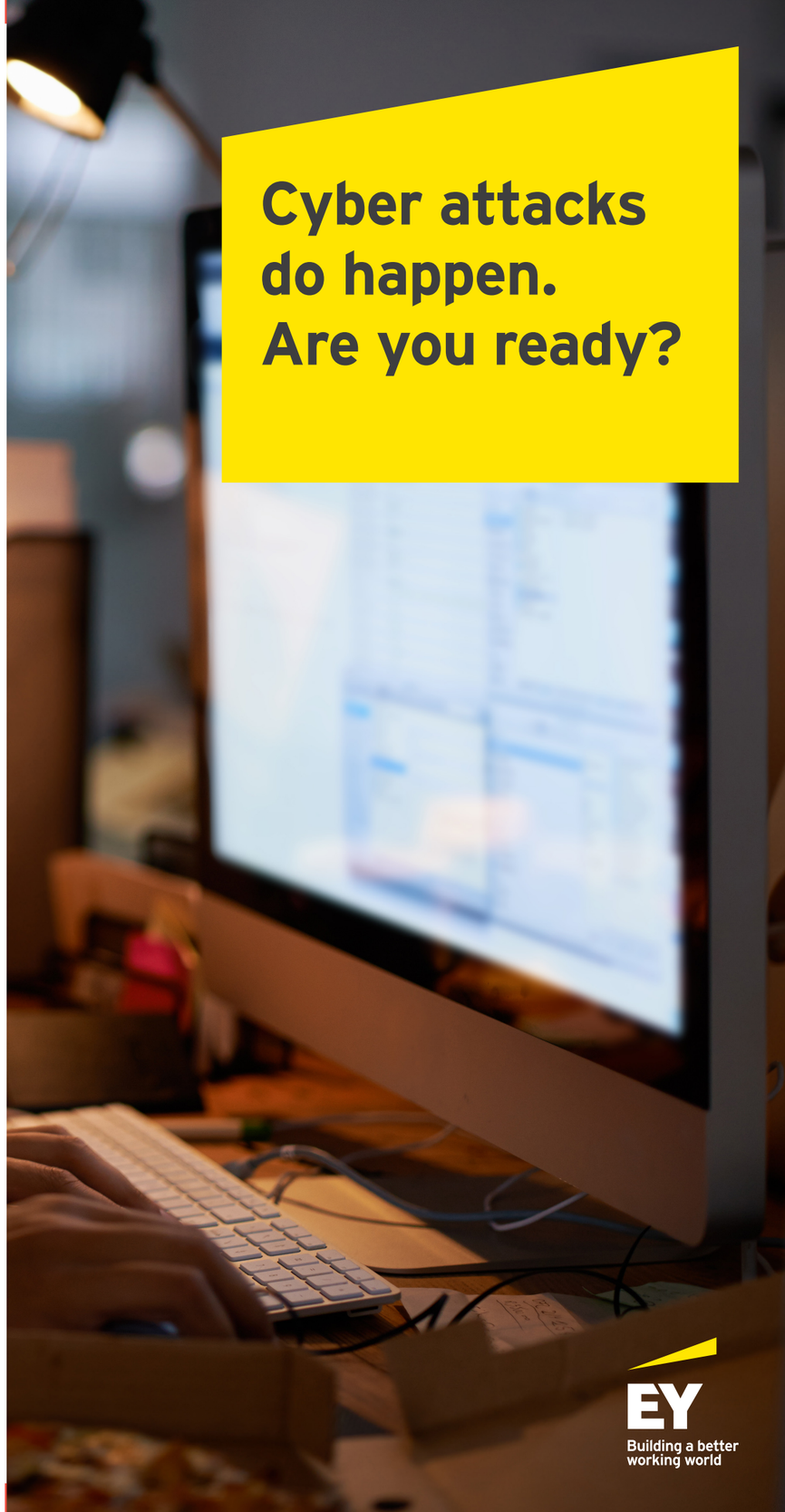
About EY's Fraud Investigation & Dispute Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the industry sector. With our approximately 4,200 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.

SCORE no. 02914-181Gbl

1804-2664290

ED None

ey.com



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.

1 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.

2 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.

Examples of incidents	
High-impact incidents and threats	
▸ Leakage of customer PII ▸ Damage to physical infrastructure and control systems ▸ Highly confidential data theft ▸ Intellectual property theft ▸ Broad malware infection ▸ Effective denial of service attack	Crisis management: ▸ Immediate involvement by the board, legal, compliance and public relations is critical ▸ Determine potential initial disclosures to external auditor, regulators, customers and third-party partners ▸ Immediately initiate the cybercrime response plan
Medium-impact incidents and threats	
▸ Unauthorized remote access ▸ Unauthorized data transmittal ▸ DMZ exposure, weak credentials	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
Low-impact incidents and threats	
▸ Misuse of computer equipment ▸ Illicit use of cloud file shares/removable storage ▸ Software piracy ▸ Access to illicit web sites	Internal investigation that is normally conducted and resolved by IT and HR

Key considerations to be prepared for a cyber attack

- A scalable approach that effectively triages and resolves incidents
- Consistent approach defined at each stage of the escalation process
- Ad hoc diagnostics and continuous monitoring
- Meaningful red flags that reduce false positives
- Address resource and infrastructure needs (e.g., training, table-top exercises, in-house vs. outsourcing)
- Insight into the risk exposure depending on the nature of the incident-disclosure obligation and compliance requirements
- Effective internal and external communication strategies

3 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 table-top 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.

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.

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.

Draw conclusions and make recommendations

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

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.

4 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.

5 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.

Inform appropriate parties

Determine what to disclose to any or all of the following:

- Regulators/law enforcement
- Auditors
- The board
- Audit committee
- Employees
- Shareholders
- Suppliers
- Customers

Increased organization-wide awareness and vigilance of cyber attack

Information security program improvement recommendations and follow-ups

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

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

Cyber threat management
- Threat intelligence
- Threat and vulnerability management
- Infrastructure and application attack and penetration
- Security operation center services
- Proactive malware identification
- Incident response

Security transformation
- Security strategy and roadmap
- Security program assessment
- Security risk assessment
- Managed security services
- Cyber economic services
- Third-party risk management

Identity and access management
- Strategy and governance
- Provisioning and de-provisioning
- Enforcement
- Review and certification
- Roles and rules management
- Reconciliation

Data protection and privacy
- Data protection strategy
- Host security
- Asset management
- Compliance and certification

Contact us at: cyberresponse@ey.com