What makes EY well positioned to help you?

- Mature cyber investigative capabilities
- Integrated, end-to-end services
- Advanced cyber analytics capabilities on big data platforms
- Dedicated industry teams
- Seasoned forensic analysts
- 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
- Understanding of the client’s organization and culture

Why EY?

"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

Are you ready?

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 more than 2,600 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.

© 2014 EYGM Limited.
All Rights Reserved.

SCORE no. WW0356
1408-1303535
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
How to respond to cybercrime

Besides an information security plan, every organization should have a strong cybercrime response plan (CRP) to assess, investigate, remediate, eradicate and respond to regulatory and other disclosure requirements. This illustration can help you implement or refine your CRP and focus on key areas.

1 Preparation
A breach 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 breach, determine whether a full-scope investigation needs to be initiated immediately.

3 Investigation
Determine how and when the compromise occurred, who was responsible 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.

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

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.

Draw conclusions and make recommendations
Develop fact patterns, and prepare report of recommendations on disclosures, program improvement and discipline.

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.

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

Information security program improvement recommendations and follow-up

Prepare for eradication events
Some remediation activities will be delayed until after the eradication event because they might tip off the attackers.

Why do companies need a CRP?
• Chances of a breach are high and alarms are going off every second, whether big or small.
• How quickly you identify and resolve a breach makes all the difference.
• Organizations need to know when and how to respond.
• There are many big stakes at risk (liability risk, compliance risk, etc.).
• Organizations need a standardized, systematic approach to resolve incidents.
• CRPs are required by insurance policies and customer or vendor contractual obligations.

Key components of a successful CRP
• A scalable approach that effectively triages and resolves breaches
• 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

Examples of incidents

<table>
<thead>
<tr>
<th>High-Impact Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leaks of customer PII</td>
</tr>
<tr>
<td>Damage to physical infrastructure and control systems</td>
</tr>
<tr>
<td>Highly confidential data theft</td>
</tr>
<tr>
<td>Intellectual property theft</td>
</tr>
<tr>
<td>Broad malware infection</td>
</tr>
<tr>
<td>Effective denial of service attack</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mid-tier threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized remote access</td>
</tr>
<tr>
<td>Unauthorized data transmittal</td>
</tr>
<tr>
<td>DMZ exposure, weak credentials</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Low-tier threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Misuse of computer equipment</td>
</tr>
<tr>
<td>Illicit use of cloud file shares/removable storage</td>
</tr>
<tr>
<td>Software piracy</td>
</tr>
<tr>
<td>Access to illicit web sites</td>
</tr>
</tbody>
</table>

- *These steps do not continue directly to step 3*