Investigation and protection from data breaches

Incident Response

kpmg.com
Data “breaches,” or the loss or potential loss of electronic information, are ever-increasing. Sophisticated, wide-scale computer attacks are becoming more prevalent. With “cybercrime” potentially threatening the operational security and competitiveness of companies large and small, no organization can afford to ignore this threat.

These attacks come from a variety of sources, including opportunistic thieves, competitors, and trusted insiders. These attacks can be traditional forms of cybercrime or even Advanced Persistent Threats (APT) carried out by highly motivated, well-funded adversaries. As a result, businesses face potential interruption of services, loss of intellectual property, and reputational damage. If individuals’ personal information is potentially lost or stolen, then a solid approach to addressing the breach can mitigate risk in a cost-effective manner.

KPMG LLP's (KPMG) Incident Response (IR) team can help your organization respond to suspected data breaches and assist you in seeking to avoid them in the future. KPMG's IR services include investigative support, intrusion detection and security monitoring, evidence collection and analysis, vulnerability assessment and remediation, expert witness testimony, and liaison with law enforcement. We can also help build your organization's IR capabilities and assist with efforts to mitigate the risk of future data breaches. For example, our professionals can assess your organization's technical and business vulnerabilities, help strategize security improvements in light of business needs, work to develop compliance programs, and assist internal audit.

KPMG's IR services are delivered through our global network of member firms in over 20 countries. Our IR services professionals possess diverse skill sets in forensics, incident response, malicious code analysis, data analytics, and network architecture. Our team has extensive experience from prior careers in military intelligence and law enforcement, some with specific experience in computer crime investigations in criminal and counterintelligence matters. They are familiar with the potential operational, financial, and regulatory impacts related to data breaches and can help clients create a response plan proactively or respond should a breach occur.

KPMG’s IR in Action

The IT help desk at an organization received reports that e-mail was down. When IT personnel responded, they discovered anomalies in a variety of operational systems, including significant impairment in security logging and a non-functional enterprise backup system. To determine if the events were the result of an intrusion or simply a series of IT-related issues, the organization’s vice-president asked KPMG to investigate.

Through the course of interviews, evidence collection, and analysis, KPMG’s IR professionals determined that the organization’s network had been breached, sensitive data had been compromised, and the e-mail of top organization officials was being actively monitored by an unauthorized source.

KPMG traced the breach to a former IT employee, and then assisted the organization’s efforts to self-report to approximately 90,000 individuals whose personal data had been potentially affected. KPMG issued a report of its findings to the organization’s board and legal counsel. This report was later provided to the U.S. Attorney’s office and the FBI to assist with prosecution of the intruder.

During subsequent months, KPMG continued to work with the organization to mitigate the risk of another intrusion by developing prioritized recommendations for improving the organization’s overall information security posture and governance.
KPMG’s Incident Response Methodology

KPMG’s IR process was created in accordance with several internationally accepted frameworks and was refined through real-world experience. It focuses on actionable results, rules of evidence, and technical security analysis and testing throughout the process. Our methodology consists of five phases:

### Prepare and Train
One of the most common causes of a failed response is lack of adequate preparation. KPMG can assist your organization in establishing clear lines of communication, policies and procedures, and rules of engagement, in order to set the groundwork for a successful response if and when an incident occurs. In a parallel track, our teams work continuously to keep current on the latest technical methods, tools, and certifications for incident response.

### Detect and Initiate
The trigger for this phase is a technical alert, an indication of fraud, or other communications from an outside entity such as law enforcement or an Internet service provider to your organization. Our IR professionals help execute plans created during the preparation phase and provide answers to pressing questions, such as: Have we been breached? Is the activity continuing? What are the potential damages? Do we need to begin notification and self-reporting?

### Contain and Investigate
During this phase, we help determine the source, method, and impact of the breach event, while attempting to assist you in limiting ongoing damage. These efforts are typically a balancing act between investigating and eradicating the threat.

### Recover
This phase consists of removal efforts that could not occur during the previous phases because of the potential impact on investigative efforts or prioritization of other activities. The focus of this stage is to return the environment to normal operations.

### Resolve
A significant work stream during this phase is vulnerability assessment and penetration testing. This work may occur throughout the IR process to support tactical efforts, and is followed by a more comprehensive process during this Resolve phase in order to determine the root causes of the malicious activity. This enables us to produce prioritized recommendations for improving the technical and governance environments, which can help prevent similar events from occurring in the future.

### Report and Pursue
The final phase consists of engagement reporting and may include ongoing support activities related to legal or civil pursuits of individuals or groups.

Responses can range from allowing the malicious actions to continue in order to facilitate evidence-gathering to an immediate suppression of malicious actions in order to limit damage.
Contact us
For more information on KPMG's Incident Response services, please contact one of our coordinators:

**Bernard Boit**  
Principal  
Forensic Technology Services  
202-533-8033  
bboit@kpmg.com

**Edward Goings**  
Principal  
Forensic Technology Services  
312-665-2551  
egoings@kmpg.com

**Greg Bell**  
Principal  
Information Protection  
404-222-7197  
rgregbell@kpmg.com

www.kpmg.com