KPMG helps major entertainment company assess recovery plan for cyber attacks

Case study

Client industry
Entertainment

Client
Global media and entertainment company

Who should read
Executives concerned about resilience against security threats from malicious hackers

Client challenge

Following the December 2014 cyber attack on Sony Pictures, our client's Chief Executive Officer (CEO) mandated a wide-ranging threat preparedness review with the aim of ensuring the company would be able to respond, that its data would be protected if key systems were contaminated by malicious hackers, and that IT operations could be recovered.

Client results

KPMG LLP (KPMG) helped the client assess the resilience of its key mission critical systems and develop a plan to mitigate risks. As a result of the review and subsequent IT system and process updates—which included addressing gaps in its backup solutions and disaster recovery plans—the company is more confident about its capacity to sustain and recover from a cyber attack.

KPMG advisor insights

Expect to be attacked

Today, cyber attacks are a major risk for organizations. The breach at Sony Pictures in 2014 highlighted the IT security vulnerabilities and lack of preparedness at many companies and prompted them to take a wide-ranging look at their recovery, contingency, and response plans.

Plan ahead

Create a thorough IT resiliency plan and maintain a strong relationship with external resiliency and forensic technology professionals who know your company and can be available on short notice to help you recover after a malicious attack.

Isolate mission-critical systems

The trend among many organizations is to place connected data centers in multiple locations around the country to enable a smooth transition in case a natural disaster or other event causes a local system failure. But with threats such as sophisticated cyber attacks that can spread malware quickly, connected highly available application solutions create a significant risk. Isolating an offline copy of mission-critical data and applications helps protect against contamination during an attack.

The project

Because of its longstanding relationship with KPMG and our involvement on other major projects, this major entertainment and media company asked us to assess its disaster recovery plans and its ability to handle a malicious attack. Our contributions included:

- Assembling a multidisciplinary team that included professionals in technology infrastructure, information protection, and forensic technology
- Identifying mission-critical applications, infrastructure services, and information that must be protected
- Identifying recovery-time objectives and recovery-point objectives for critical services that could be affected by a cyber attack
- Identifying and documenting potential gaps in the company's disaster recovery plans
- Recommending steps to address gaps and threats to its core applications and services.
- Assessing offline backup and restoration capability for in-scope applications and services.

If you are interested in learning more about this case study, or if you are experiencing similar issues, please contact us.

David Tarabocchia
Managing Director, CIO Advisory
KPMG in the US
T: 813-301-2104
E: dtarabocchia@kpmg.com

www.kpmg.com/us/IT