IIA Bulletin

The Institute of Internal Auditors

Perspective for internal auditors on today's most urgent issues *February 2020*

RETHINKING PREPAREDNESS: PANDEMICS AND CYBERSECURITY

The coronavirus epidemic is bringing into sharp focus an issue that is often overlooked by organizations — business continuity and disaster preparedness.

Uncertainty about the scope and duration of the current epidemic is already making an impact, from organizations re-evaluating employee travel plans to jittery investors selling off stocks. With the potential to affect supply chains, worker productivity, and third-party relationships, the risk of an expanding outbreak should be on the minds of business executives and internal audit leaders alike. At a minimum, internal audit leaders should be prepared to review and recommend necessary updates to pandemic, disaster preparedness, and business continuity plans.

Even as organizations are in the first stages of determining the potential impacts of the coronavirus on their operations, an ancillary risk is emerging — social engineering amid crisis. Cybercriminals are taking advantage of the growing concern over the deadly virus. Malware-laced emails masquerading as guidance about the virus turned up in three Japanese prefectures, according to TechRadar Pro, a UK-based consumer technology news and reviews website. Hackers disguised the malware in email attachments purporting to contain information to protect against spreading the virus. Instead, they were laden with a virus of another kind, according to TechRadar Pro.

Cybercriminals taking advantage of crises is something that likely will become more prevalent. Organizations must build up their protocols and practices to defend against social engineering such as phishing, pretexting and baiting.

General questions to assess your organization's disaster preparedness

The following are some general questions your internal audit department should ask to determine if your organization is properly addressing disaster preparedness and business continuity planning:

- When was the last time your organization's resiliency plans were reviewed by key stakeholders? When was the last time your organization's plans were tested and by whom?
- How do your current plans address natural disasters, pandemics, or other potential disruptors that could impact your facility? Your employees? Your cloud providers? Your suppliers? Your customers?

- When was the last time your organization reviewed its contracts with business resiliency partners?
- How are vendors, emergency responders, regulators, insurance agencies, and other critical stakeholders notified of point of contact changes?
- How capable is your organization to perform manual versions of business-critical automated activities? Are the needed forms and procedure manuals available? Are you appropriately staffed to do so?
- How often does your organization verify the criticality of various business processes to make sure the order of recovery is appropriate? How does IT ensure the critical infrastructure components are enabled to allow for the business recovery requirements?
- What business objectives would be hindered or restricted if there was limited or no internet or cellular access?
- What training have your employees and business associates received on what to do in the event of a natural disaster or a pandemic?
- Is your data center and/or your cloud provider capable of running "lights out," meaning no workers present for an extended period?
- What business-critical processes or activities would not be transferrable to an alternate location? Which have regulatory implications based on timing or duration of event?

General questions to assess your social engineering vulnerabilities

The following are some general questions your internal audit department should ask to determine your organization's vulnerability to social engineering schemes:

- What are your organization's practices, policies, and training involving the threat of social engineering? How are these communicated to employees and enforced?
- Is the threat of social engineering completely understood and communicated to all levels of employees at your organization?
- Which systems and processes are particularly vulnerable to social engineering? Which key business processes have potential to be affected?
- What testing does your IT department do relating to areas of specific vulnerability to social engineering?
- Do you have plans to audit your organization's areas of specific vulnerability to social engineering?

IIA RESOURCES

Knowledge Brief

- Strategic Public Asset Protection

Practice Guides

- Assessing the Risk Management Process
- Auditing Third-Party Risk Management
- Coordination and Reliance: Developing an Assurance Map
- Business Continuity Management
- GTAG: Business Continuity Management
- GTAG Assessing Cybersecurity Risks

Internal Auditor magazine

- In the Face of Nature

ABOUT THE IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters are in Lake Mary, Fla. For more information, visit www.theiia.org.

COPYRIGHT