IIA Bulletin

The Institute of Internal Auditors

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

PANDEMICS: CONSIDERATIONS FOR IT DISRUPTIONS

The COVID-19 pandemic has forced the business world into unplanned workarounds in operations, which in turn have spawned a unique set of risks. This is particularly true for cyber risks. While operational changes related to social distancing and stay-at-home mandates continue to manifest, IT resources are being redirected to support telecommuting, expanded video conferencing, and associated troubleshooting. As IT professionals pivot to address these new demands, organizations could be exposed to novel cyber threats and vulnerabilities or, worse yet, lose focus on existing threats.

Among the most troubling is the risk of "zero-day" exploits. The term describes cyberattacks that occur when a weakness is discovered in a particular software, firmware, configuration setting, or operating system that is unknown to the developer and has no known or recommended remediation. Such security weaknesses or vulnerabilities are unknown or unexpected consequences that often result from programing errors or improper computer or security configurations. The threat is twofold; cybercriminals can exploit the vulnerability until a patch is available in the short term, but this becomes a long-term threat if the recommended guidance or patch is not implemented as soon as it is available.

One important task internal auditors can perform right now is an assessment of the full impact of the pandemic's impact on IT resources, priorities, and focus. It should include determining whether the current procedures in place to keep IT up to date and aware of potential zero-day attacks and other vulnerabilities are sufficient and effective.

General questions to assess cyber vulnerability during the COVID-19 crisis

1. How does the organization monitor trusted news outlets and other information sources in regards to potential zero-day exploits? Has the process for dealing with these risks changed?
2. How does the organization ensure necessary security-related patches are being implemented in a timely fashion?
3. Have any threat hunting (proactive cyber defense activities) or other monitoring or scanning activities been altered because of changes in the organization's processes and work environment? How are any resulting risks addressed?
4. How is the organization ensuring vulnerability management practices are being properly administered as a result of changes to the work environment? What specific vulnerability scanning or remediation activities have been altered or postponed?

5. How does the organization ensure IT incident management practices — including procedures to prevent, detect, and respond to incidents — are up to date with latest threats? How does IT continue to ensure current processes include the tools and services needed to triage, analyze, contain, eradicate, and respond to an event?
6. How does the organization ensure changes to the network are properly requested, documented, approved, and executed? This specifically includes emergency or ad-hoc changes made to facilitate remote operations.
7. How have the organization's physical and logical access provisioning processes changed? Has the change in the work environment postponed entitlement reviews or provisioning procedures for additions, transfers, and terminations?
8. What critical processes cannot be performed or monitored in a remote work environment? How are any resulting risks addressed?
9. How has the pandemic response changed vendor relationship management, including relationships with major cloud vendors?
10. What changes have been implemented in regard to contract management? For example, have contract requirements been relaxed or bypassed?
11. How has the procurement process changed as a result of changes to the work environment? Specifically, what is being done by the organization to address the potential increase of user-acquired or implemented systems, applications, and services?

IIA RESOURCES

Practice Guides

- GTAG: Business Continuity Management
- Practice Guide: Business Continuity Management
- GTAG Assessing Cybersecurity Risks
- Practice Guide: Assessing the Risk Management Process
- Practice Guide: Auditing Third-Party Risk Management
- GTAG – Insider Threats

Training on Demand

- Auditing Insider Threats OnDemand