Riskigy vCISO Team Resources: Cybersecurity Tabletop Exercise Series

Our Scenarios to Help Prepare Your Incident Response Team

Exercise Title:

Leaky Printer

TTE Scenario:

A large number of confidential documents have been discovered online. Despite conducting comprehensive network scans, no indications of compromise have been detected. However, it seems that the multifunction printer/copier is linked to an external IP address. All of the documents discovered on the Internet were confirmed to have been printed or duplicated using this machine. The device was not initially linked to the Internet, but it has since been connected through a Cat5 cable.

Cyber Attack:

It is possible that this situation could be a result of a data breach or unauthorized access, resulting in compromise to the multifunction printer/copier connected to the Internet. It's also possible that the confidential documents were mistakenly shared or uploaded to an online platform.

Incident Impact:

- Organization disruption: A device compromise can disrupt organization operations, resulting in downtime, lost productivity, and potential revenue loss.
- Cybersecurity posture degradation:A device compromise can erode the overall cybersecurity posture of an organization by exposing weaknesses in its security controls and processes, making it more vulnerable to future attacks.
- Cybersecurity liability: Insurance may or may not cover the compromise situation, depending on the damage caused.
- Malware: When staff members who are not properly trained connect untrusted or unauthorized devices to company computers and networks, it can lead to the introduction of malware.

Lesson to Learn:

- How can you determine the severity of the leak?
- How can you assure it doesn't happen again?
- How do you find out what kind of information was processed by this printer?
- How do you check printer logs?
- Does your organization have employee training to reduce this threat?

Riskigy