Riskigy vCISO Team Resources: Cybersecurity Tabletop Exercise Series

Our Scenarios to Help Prepare Your Incident Response Team

Exercise Title:

The Accidental Insider Threat(s).

TTE Scenario:

Your accounting and finance team recently visited the annual conference tradeshow of "QuickSuiteTree accounting software" and was provided a gift basket of gadgets and goodies by the host.

A malware infection outbreak caused by a malicious payload carried on promotional devices the accounting team received from their financial accounting software service provider.

Cyber Attack:

Cybercriminals have infiltrated a manufacturer of USB gadgets such as USB desktop fans, lamps, and picture frames. The gadgets are distributed around the world with various logos, branding and marketing swag in goodie bags at tradeshows and conferences.

Incident Impact:

- Untrained staff may introduce malware when connecting unauthorized and untrusted devices to company computers and networks.
- Breach impact can vary depending on the staff and data compromised. Staff in financial accounting, human resources and others have access to data which is always considered confidential and high sensitive.
- A lack of visibility on endpoints may delay identifying unauthorized devices or attempts at unrestricted access to computers and/or services.
- Cybersecurity liability insurance may or may not cover incidents caused by employee social engineering attacks such as fund transfer and fraud.

Lesson to Learn:

- How would your organization identify and respond to suspicious activity on your systems through this vector?
- What resources (staff, contractors, partners) could present similar threats?
- Who within the organization would you need to notify?
- How can you prevent this from occurring at your organization?
- Does your organization have employee training to reduce this threat?

Riskigy