FORTINET

Three Simple and Effective Cybersecurity Exercises

John Hollenberger

Senior Security Consultant, Proactive Services

John Hollenberger

Senior Security Consultant, Incident Response

jhollenberger@fortinet.com

N/A

hollenberger

Pittsburgh, Pennsylvania

CISSP, CISA, CISM, CRISC, GCIH, GWAPT, Security+

Fortinet USA
899 Kifer Road
Sunnyvale, CA 94086
United States

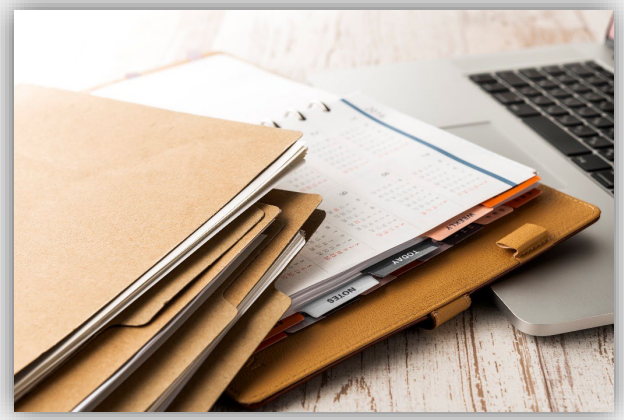
- Over 15 years of experience in cyber security and IT Operations, including four years as the Director of IT for a non-profit organization.
- Previous focus areas include web- and host-based vulnerability assessments, incident response, PCI compliance and Data Loss Prevention.
- Passion for investing in the education and training of peers in the security industry.
- Presented, trained and mentored on proactive Incident Response services for large corporations, small businesses, and non-profit organizations. Presented at a number of national and regional conferences.
- Serves as a local volunteer firefighter.

Goals of Today's Presentation

Cybersecurity Exercises can be Easy!

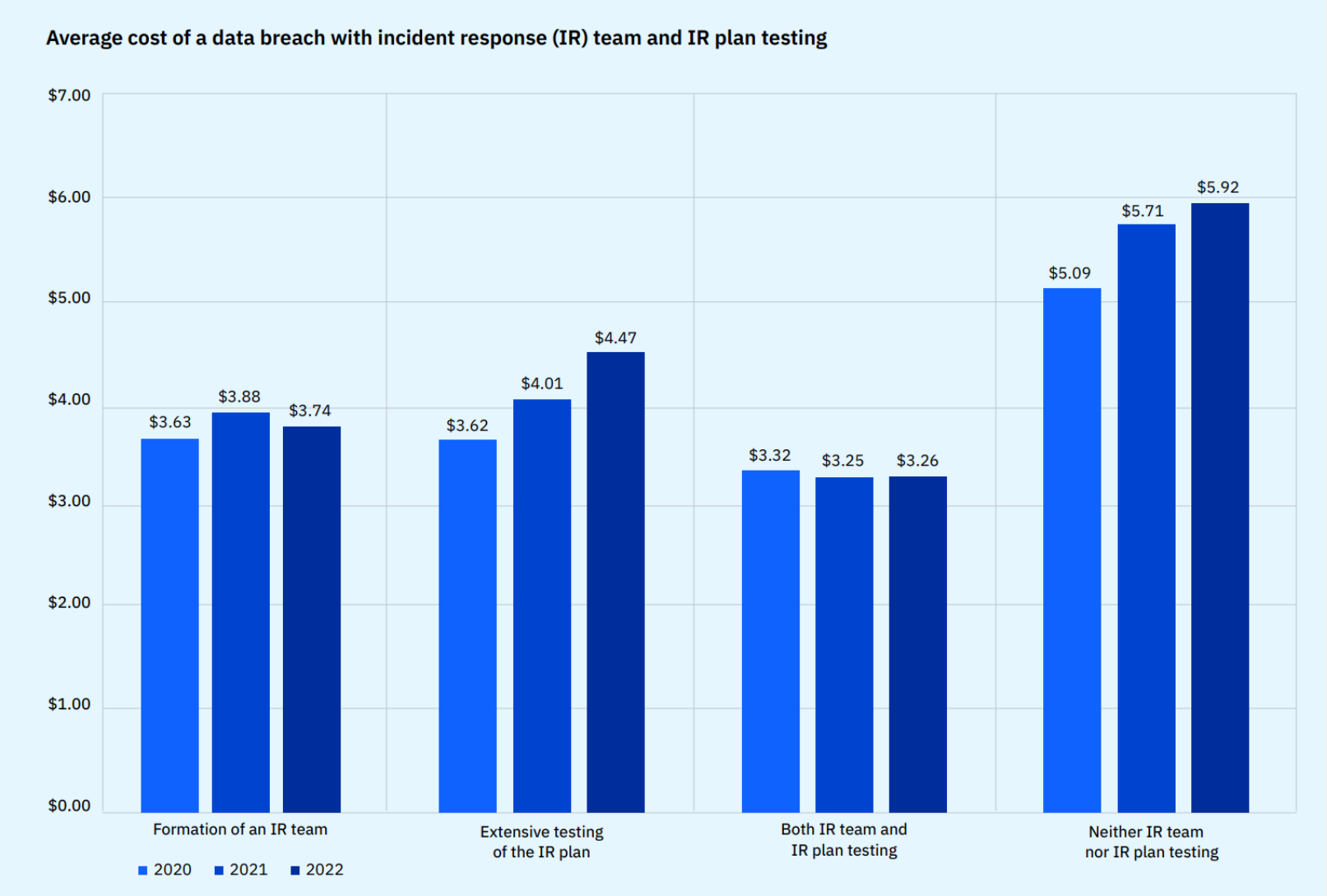
- Cybersecurity exercises do not need to leverage complex, lengthy scenarios.
- "Simple" is just as good, if not better.
- Takeaway three simple exercises which are applicable to most organizations.

Why Perform Cybersecurity Exercises?



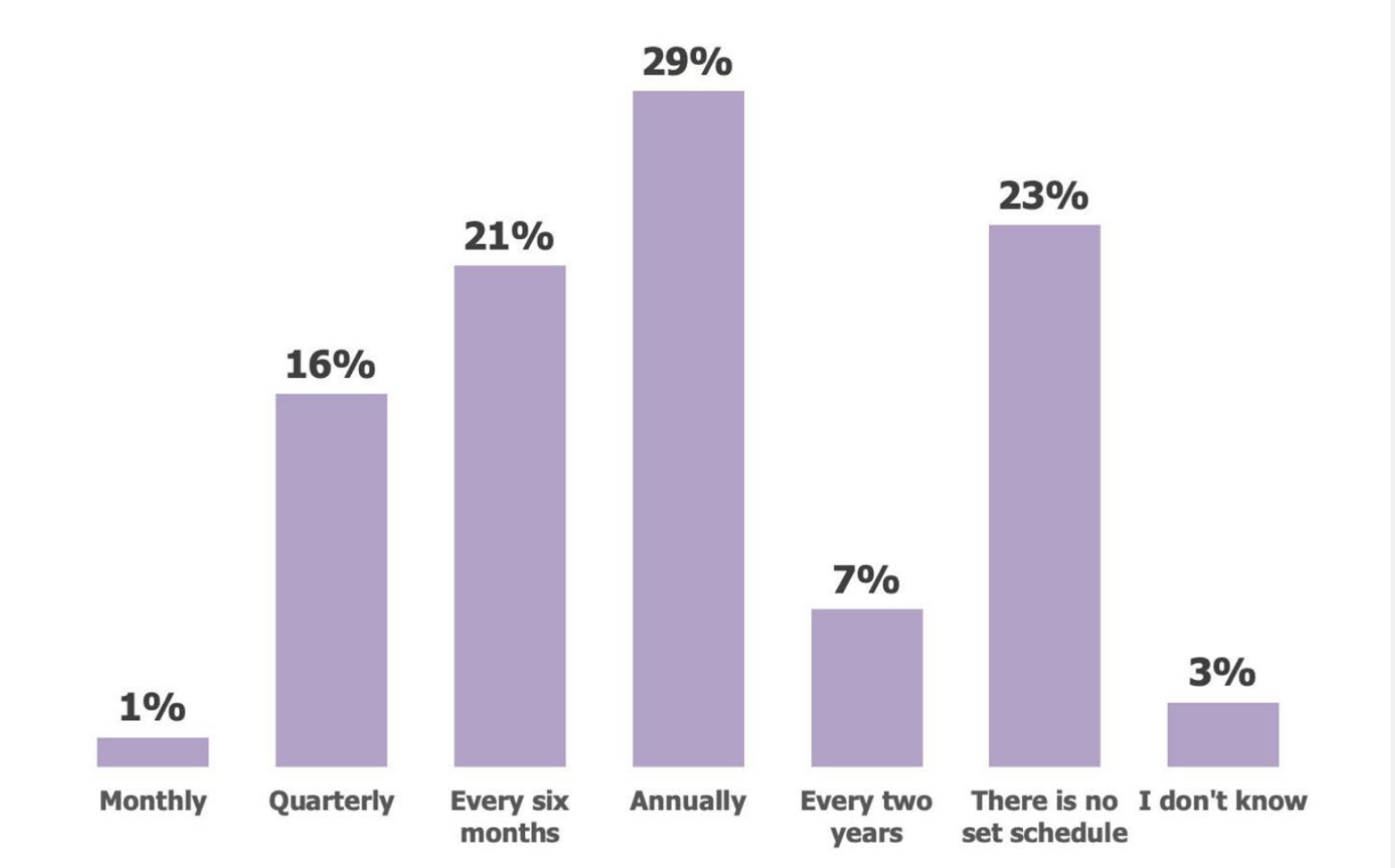
Average Total Cost of a Data Breach with an IR Team and Plan Testing

Measured in USD - Millions



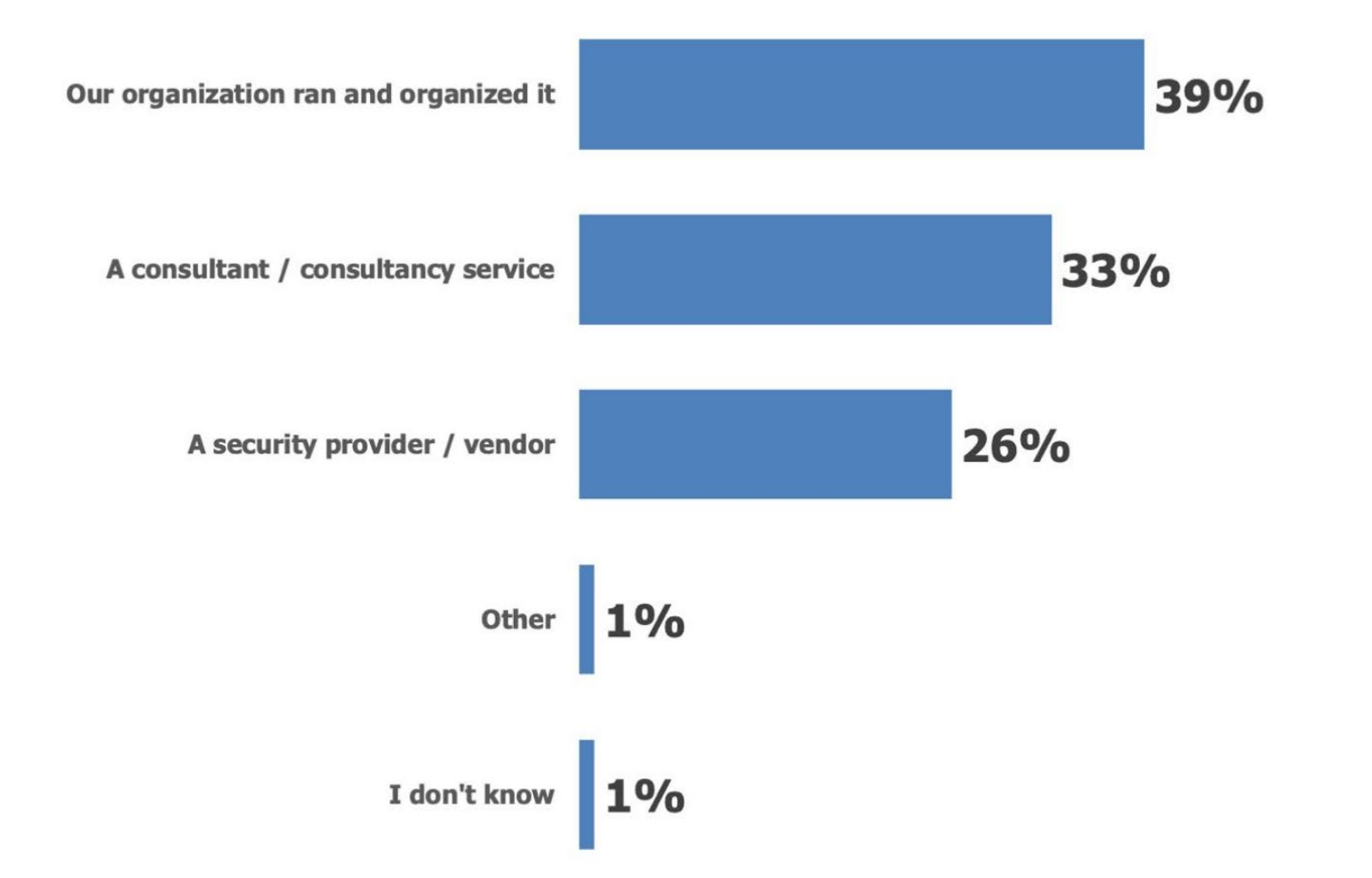
Source: Ponemon Institute & IBM Security | Cost of a Data Breach Report 2022
Used with Permission.

Frequency of Tabletop Exercises



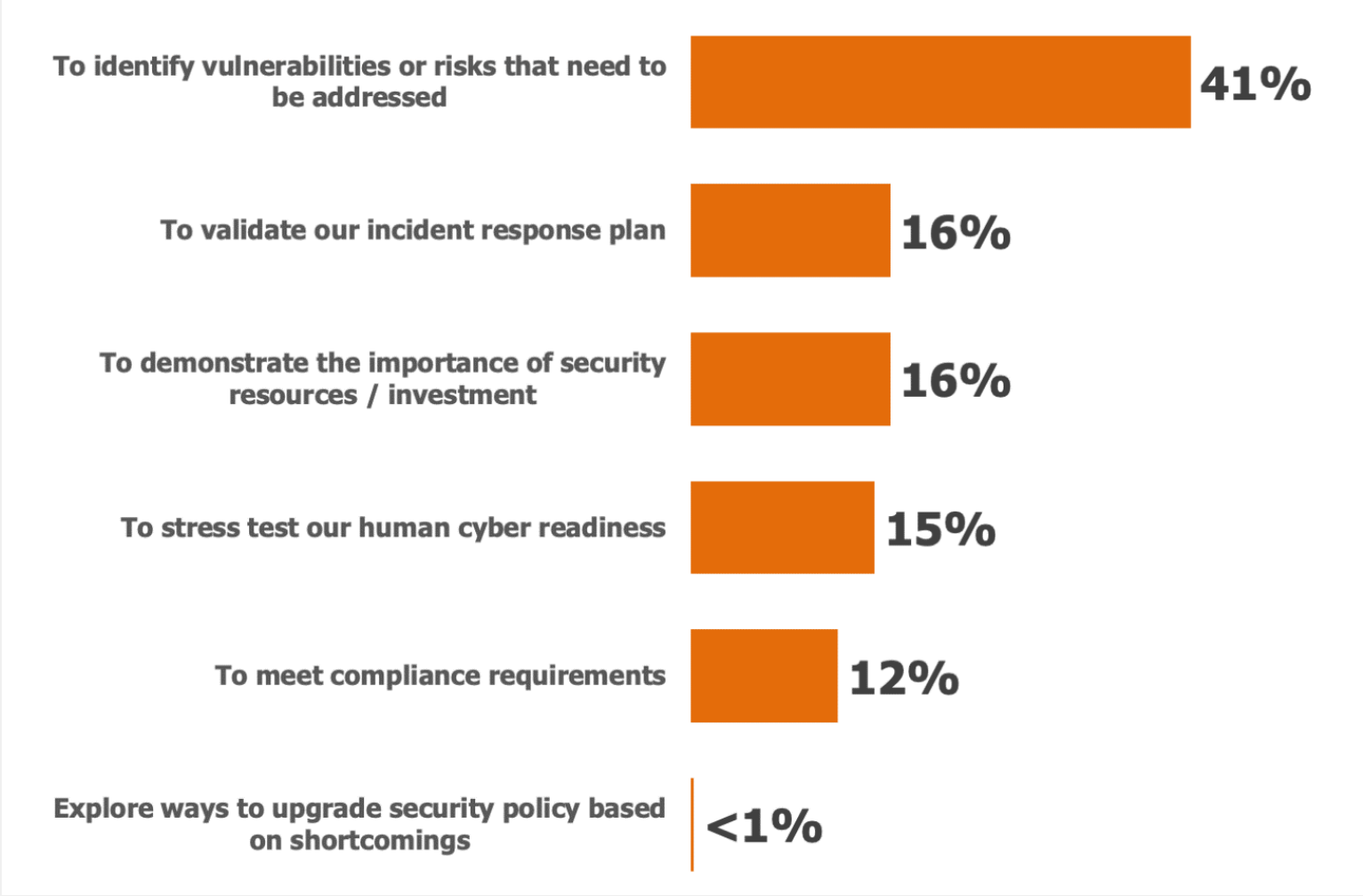
Source: Osterman Research and Immersive Labs. 2020.
Used with Permission.

Primary Organizer of the Most Recent Tabletop Exercise



Source: Osterman Research and Immersive Labs. 2020.
Used with Permission.

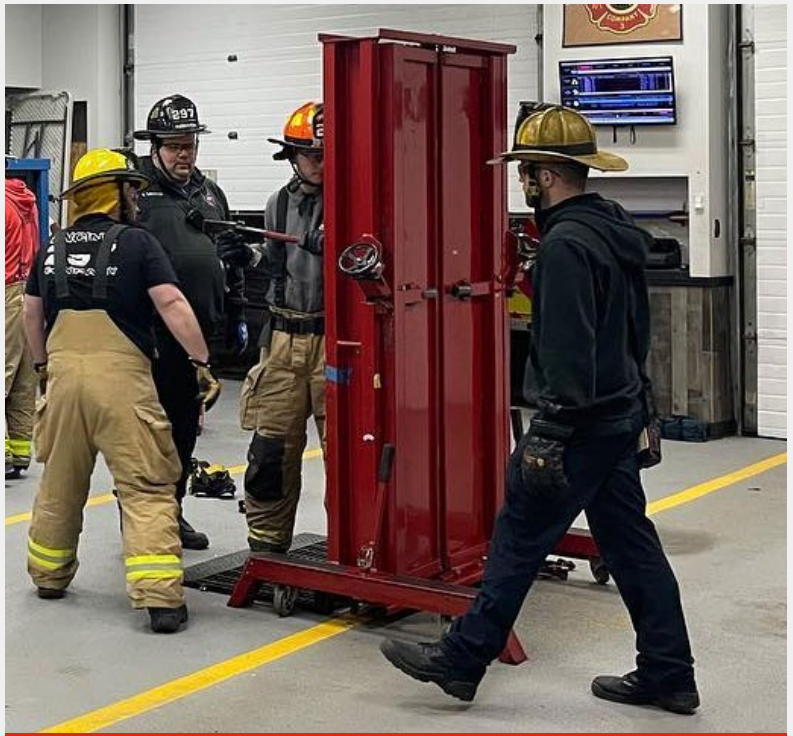
Motivations for Running a Tabletop Exercise



Source: Osterman Research and Immersive Labs. 2020.
Used with Permission.

Types of Exercises

Tabletop Exercise



Drill

Functional Exercise

Exercise 1: Social Media Compromise

Audience:

- Executive
- Cross-Functional
  - Communications
  - IT
  - InfoSec
- Physical Security

Exercise 1: Social Media Compromise

Goals:

- Understand roles and responsibilities within the organization.
- Focus on internal and external communication requirements.
- Understand external resources that will need to be brought in.

Discussion Points:

- Social media security practices.
- Internal and External stakeholder Communications.
- Media relations / law enforcement relations.
- Alternative means for communicating (i.e., no social access).

Exercise 1: Social Media Compromise

Variables:

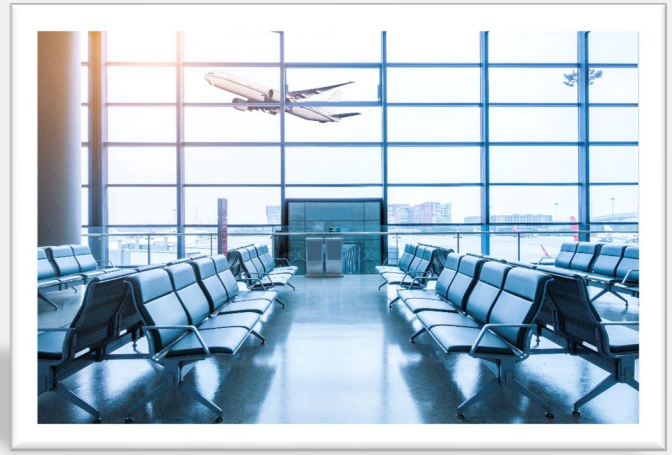
- Multiple channels lost (e.g., Facebook, Twitter, LinkedIn).
- Posts go viral.
- Inquiries from regulatory authorities.
- Postings release sensitive data.
- Social media platforms take 48 hours to regain control.
- Attacker gains access to parts of the network.

Exercise 2: The Lost Laptop

The organization receives a call from TSA Agent, Droopy Carmello.

He advises that:

“A laptop was found and the asset tag on the device said to call this number if found.”



Audience:

- Hardware/Asset Management
- Data Loss Prevention
- Information Security
- Marketing/Communications
- Physical Security

Exercise 2: Lost Laptop

Goals:

- Focus on data classification within the organization.
- Ensure proper escalation of information and communications to the appropriate teams/individuals.
- Understand roles and responsibilities based on actions needed.

Discussion Points:

- Release of sensitive information.
- Disciplinary action.
- Laptop retrieval.
- Extent of compromise.
- DLP technology.
- Regulatory requirements.

Exercise 2: Lost Laptop

Variables:

- Laptop was on and logged in.
- Laptop belongs to a high-level executive.
- Contains unreleased earnings information.
- Employee is a repeat offender.
- Laptop found by nefarious actor that is attempting to extort the organization.

Exercise 3: Hands on Drill

HR and Legal schedule an unexpected meeting.

“We need an image of all of Michelle Murray’s laptop, including any drives plugged in. While we cannot provide further details at this time, here is a written and signed agreement from legal providing you authority to proceed.”

“Please know this may end up in court so chain of custody is crucial.”

Audience:

- Technical Resources
- Incident Response
- Third-party forensics team
- Legal
- HR
- CISO

Exercise 3: Hands on Drill

Goals:

- Disk image created of internal SSD and external HDD.
- Memory dump completed of laptop.
- Proper chain of custody followed.
- Ensuring confidential communication maintained throughout the exercise.

Discussion Points:

- Skillset available to collect the evidence.
- Tools needed for imaging.
- Chain of custody.
- Time to complete.
- External forensics provider.
- Documentation and workflow.

Exercise 3: Hands on Drill

Variables:

- Nobody within the organization has experience with forensics tools.
- Unsure of how to maintain chain-of-custody.
- Employee learns of the investigation (and not from HR or legal).
- Employee wiped their computer and hasn't shown up for work in two days.

Keys to Success

- Keep it simple.
- Don’t overthink the exercise.
- Set clear goals.
- Practice often.

Questions

John Hollenberger

jhollenberger@fortinet.com

←This is probably legitimate ☺


FORTINET