Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

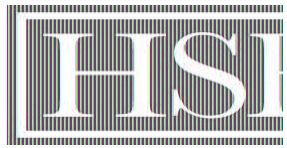
This is NOT a Drill: The Importance of Incident Response Testing

Rochester Security Summit

October 25, 2023

Dan Altieri, Esq.

Laura K. Schwalbe, Esq., CIPP/US, CIPP/E



Agenda

- IR and TT Introduction and Background
- The What
- The Why
- The How
- Closing Thoughts/Questions

Backbone of IR: Incident Response Plan

- What is it (and what is it NOT)?
- Core Components from NIST SP 800-61
  - Preparation
  - Detection and Analysis
  - Containment
  - Eradication
  - Recovery and
  - Post-Incident Activity
- What's not listed in NIST SP 800-61?
  - Communications
  - Privilege
  - Third Parties
  - Insurance
- Team roles and responsibilities

The What: Incident Response Plan

- Structure and flexibility
  - Not every answer to an incident will be in the IRP
  - Too much specificity will make an IRP immediately obsolete
- Primary audience is not IT
- Communication is key, and risky!
  - Incident Response Plan, not *Breach* Response Plan

The Why

- Test Plan and Train the Team
- Learn Something (Hopefully!)
- Identify Areas for Improvement
  - Table Top Informs Risk Assessment

The Why ctd.

- Legal Framework
  - SHIELD Act
  - NYS DFS Proposed Amendment
- Insurance policies and applications
- Etc.!

The How

- An event will be described in broad terms.
- As time progresses, the incident will unfold.
- Much like a real incident, not all information will be available. There will be unknowns!
- Standard rules of engagement

The How: Pick Your Scenario

- Do your homework
- A good scenario addresses:
  - Detection, triage and escalation processes
  - Resource availability
  - Internal and external communications
  - Downtime procedures
  - Third party engagement
  - PR issues, and more . . .

The How: Pick Your Scenario ctd.

- Ex. Ransomware:
  - Ransom note discovery
  - Impact of encryption … and exfiltration?
  - Dealing with the cyber criminals and ransomware resolution services
  - Law enforcement interactions
  - Threat actor scare tactics
  - Do you pay?

The How: Privilege and Staffing

- Tabletops and IRP testing should be done under privilege
- Allow for full and frank discussion of potential problem areas
- Who has a seat at the table?

The How: Insurance

- If you don't have it, you likely need it, but all forms are not created equal
- If you have it, you should spend some time figuring out what's in it
  - Proactive Processes (like IRP testing, tabletops)
  - Exclusions
  - Network extortion
  - First and third party losses
  - Notice requirements
- A good broker matters

The How: Beyond a Tabletop

- Vulnerability Assessments
- Penetration Testing
- Risk Assessment
- Policy and Procedure Review
- Training

Questions?

Thank you!

Harter Secrest & Emery LLP

ATTORNEYS AND COUNSELORS

WWW.HSELAW.COM

ROCHESTER • BUFFALO • ALBANY • CORNING • NEW YORK CITY