CYBER CLAIM TABLETOP EXERCISE

Meredith Quick

Senior Director of Risk Management
NextEra Energy, Inc.

Melissa Ventrone, Esq.

Partner
Clark Hill PLC

Jason Dely

Technical Director, Industrial Control Systems
Cylance, Inc.

Thomas Pace

Senior Director, Worldwide Consulting
Cylance, Inc.

MODERATED BY

Dawn Simmons

Vice President – Underwriting, Cyber
AEGIS Insurance Services, Inc.

AGENDA

- Purpose and scope of a cyber Incident Response Plan (IRP)
- Importance of a tabletop
- Why responding well matters
- Identification of an event and triggering the incident response team – whose responsibility is it anyway?
- Good practices, lessons learned from others
- Security incident simulation exercise

Imagine someone trying to break into your house.

Now imagine it
60,000 times a day.

http://www.ibm.com/smarterplanet/ie/en/business_resilience_management/overview/index.html?re=spf

IMPORTANCE OF A CYBER INCIDENT RESPONSE PLAN

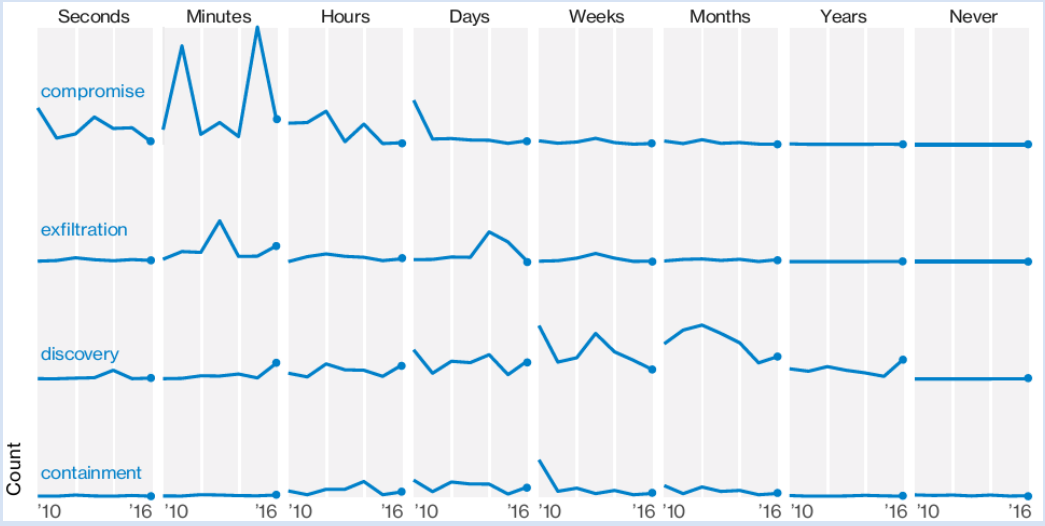
- What is a cyber IRP?
  - An organized approach to addressing and managing the aftermath of a cyber incident or cyber attack of computer systems that could result in data breach, security breach, or system interruption
  - Goal is to manage a situation in a way that limits damage and reduces recovery time and costs
- Importance of incident response
  - Enables an organization to be prepared for the unknown as well as the known
  - Reliable method for identifying a cyber incident immediately
- An IRP should include procedures to detecting, responding to and limiting the effects of a cyber incident

AEGIS 2018 PHC

SCOPE OF A CYBER IRP

- Identification of the threat or security incident
  - What just happened?
    - Triggering the incident response team
  - Making sure the right people / partners are a part of the team
    - Containment
  - Have you stopped the "bleeding"?
- Remediation
  - Have you taken steps to prevent this type of event from occurring in the future?
- Notification – and beyond
- Identification: time to **impact** vs. time to **discover**

TIMESPAN OF BREACH EVENTS OVER TIME



Source: Verizon's 2017 Data Breach Investigations Report, 10th edition

AEGIS 2018 PHC

THE MISSING LINK: FROM POLICY TO IMPLEMENTATION

- You've drafted an IRP – now what?
  - Have the policy reviewed by all departments and key incident response team members
  - Let people know they are on the incident response team
    - How do you activate the team?
    - How quickly are team members required to respond?
    - What happens if someone is unavailable?
    - Who is the spokesperson for the team?
    - What if the spokesperson is unavailable?
- A plan never survives first engagement with the enemy

LIFE CYCLE OF AN INCIDENT

Identification → Containment → Remediation → Notification

- Triggering the incident response team
  - Identifying that an event has occurred and determining who needs to be involved
- Stop the bleeding – but don't damage the wound!
- Taking steps to prevent a similar event from occurring in the future
- Who do you tell?
- How?
- When?

WHY RESPONDING WELL MATTERS

- Miscommunication can be catastrophic
- A delay in investigation and response can be catastrophic
- As can responding too quickly

STUMBLING BLOCKS – WHAT ARE THEY?

- The buck stops here – who has ultimate authority to make the decisions?
- External communications – difficulty involved
- Identifying key stakeholders
- Identifying the “extras” that will expedite the response process

PURPOSE OF A TABLETOP EXERCISE

- Objective-based exercise
  - Tabletop simulations provide a great vehicle for organizational awareness and training for inevitable security incidents
  - Allows a team to come together in a low-stress environment to assess their procedures and plans
  - Test the incident response plan to determine strengths and weaknesses of plan
- Scenario
  - Relevant to company threats and environment (asked to not fight the narrative)
  - Plausible based upon based on industry known incidents
  - Inclusive of all participants
  - Solvable by the team assembled
  - Scenario injections introduced to evolve the situation and support to achieve exercise objectives

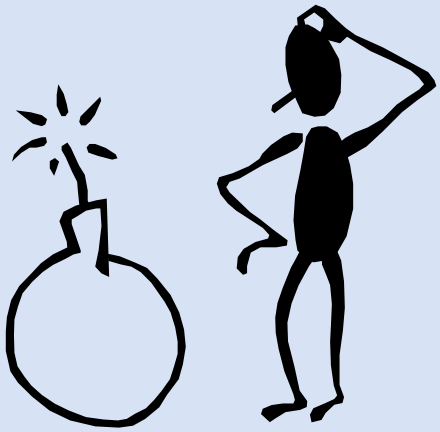
TYPE OF EXERCISE

- Tabletop exercises
  - Facilitated, discussion-based exercises of a given scenario
- Functional exercises
  - Validation of readiness through performance of duties in simulated environments
- Tool evaluation
  - Validation of operability of system components with quantifiable metrics
- Control validation
  - Technical or procedural control validation using active introduction of simulated attacks

DATA BREACH EXERCISE RULES OF THE ROAD

- There are no wrong answers
- More participation equals more fun
- Don't be afraid to "what if" the participants
- Ask questions throughout
- Liberal application of fairy dust!

CYBER ATTACK



SIMULATION EXERCISE

- Things are going smoothly, until…
  - At 8:30 am on Friday, IT receives a complaint from an employee that he could not access key business-critical applications and documents

CURRENT STATE OF ENVIRONMENT

- Background on systems
  - The business-critical applications are hosted by an outside service provider
  - Your point of contact is a relationship manager
- Your access to the system is limited to entering data, assigning / terminating accounts, resetting passwords, running reports
  - Security, integrity and availability of data and applications
  - Contract simply says provider is required to have adequate back-ups

WHAT DO YOU DO?

- Contact the relationship manager
  - You reach their voicemail
  - You call the help desk number, which forwards you to a call center that promises to forward your inquiry to an emergency number
  - Four hours pass before someone returns your call

PROVIDER RESPONSE

- You reach the relationship manger, who tells you
  - Their entire system has been hit by a ransomware attack
  - They are working to restore the system
  - They will be in touch shortly
- Now what?

RANSOMWARE

- When ransomware affects vendors' systems
  - Service level agreements usually do not anticipate this type of event
  - Depending on size of vendor, the system will most likely be down for several days
  - Contracts do not contain sufficient cyber security audit requirements

WHAT IF IT IS YOUR SYSTEM?

- Responding well matters
  - To pay or not pay, that is the question
    - You have to have adequate backups, can restore from backups, to limit downtime
    - **What if backups are infected as well?**
- What if you don't have backups
  - Attacker accessed your system, turned off the backups
  - Backups configured wrong
  - Backups infected as well

RANSOMWARE RECOVERY

Options

Pay for decryption key

Restore from backup

RANSOMWARE RECOVERY

- **Pay for decryption key**
  - Create forensic copy of affected devices
  - Test encryption key on data, then execute
  - Review device to make sure no secondary infection is present
  - Restore clean devices
- Conduct legal analysis
- Determine if incident is reportable to clients, regulators, or individuals

RANSOMWARE RECOVERY

- **Restore from backup**
  - Run scans on backups to make sure they are not infected as well
  - Upload signature to anti-virus provider, run it across network
  - Confirm no secondary infection
- Conduct legal analysis
- Determine if incident is reportable to clients, regulators, or individuals

RANSOMWARE EVENT

- What does this mean?
  - Test your systems, test your backups
  - Make sure your vendors test their systems and backups
  - Review contracts carefully to protect your interests

RANSOMWARE EVENT

- In summary
  - Preparation is key to responding to an event successfully
  - Practice – the worst time to test your incident response plan is in the middle of your first incident

AEGIS