VAPDC WINTER SERIES

Confronting Cyber Challenges

Friday, March 3, 2023

Guidance Overflow = SO MUCH INFO ⍰

- Cyber Incident Response | CISA
- Stop Ransomware | CISA
- National Cyber Awareness System | CISA
- MS-ISAC (cisecurity.org)
- Cyber Incident Checklist (cisecurity.org)
- Computer Security Incident Handling Guide (nist.gov)
- Preparing for a Cyber Incident (secretservice.gov)
- Ad infinitum…

>> BUT, the good news is, it all relates and it all “works”

Where to start?

NIST or CISA or CIS or VDEM or Secret Service of FBI or ⍰♂

1) Just pick one to start

2) Use what works for you

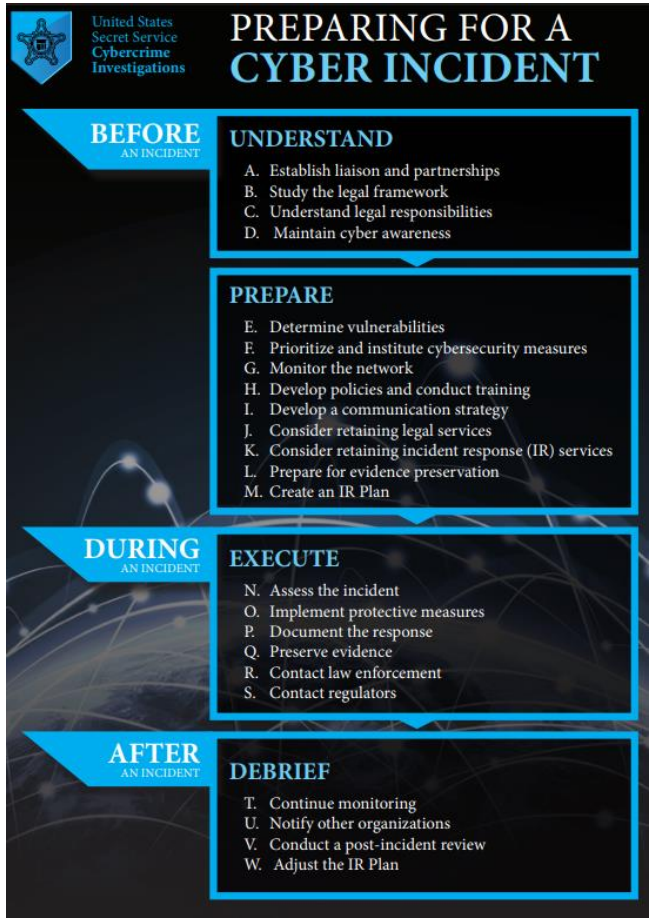
3) Cover the basics

4) Use available support

VDEM Core

NIST CSF
(COVIT Core)

≈



The Incident Handling Process

Preparation

- **Definition:** *Proactively addressing known needs should a cyber incident occur*

- Identify an incident manager prior to incident
- Complete security triage questions
- Establish network map
- Implement asset identification and configuration management
- Turn on logging
- Follow an established cybersecurity framework
- Routinely conduct and verify offline backups
- Complete MOUs and NDAs for assistance (VANG)
- Education of staff & executive level awareness
- Exercise good supply chain management

Identification

- **Definition:** *Identifying the malware, attack vectors, and system pivoting associated with a specific cyber incident*

- Contact Virginia Fusion Center for resource assistance
- Forensic imaging of known affected devices (can be conducted by VSP)
- Images can be analyzed while containment begins
- VSP installs network tap with permission of locality in order to capture traffic
- VFC, in conjunction with other partners, conducts log/artifact analysis

Containment

- **Definition:** *Stopping the bleeding*

- Remove affected devices from network but do not power them down
- Software & hardware hardening
- Closing unnecessary or unused ports
- Disabling or removing unknown or suspicious accounts
- Decouple domain and local admin accounts from user accounts
- Quarantine and/or adjust network rules to prevent communication with command and control
- Geoblocking locations as appropriate
- Forced password resets

Eradication

- **Definition:** *Eradication is the elimination of the malware and corr-ection of processes that allowed & sustained the attack*

- Proactive deployment of software for the purpose of eradication
- Restoring from known, good patched backups
- Disabling unnecessary services on network

Recovery

- **Definition:** *The process by which networks are returned to full operation*

- Utilization of procurement framework to obtain expedited equipment
- Acquisition of assets as necessary to be used as a temporarily deployed mobile infrastructure until permanent equipment is obtained
- Post incident assessment conducted by VANG, VDF, or CISA

Lessons Learned

- **Definition:** *Create space to conduct a post-incident analysis to identify areas of improvement*

- Identify processes that should be improved to prevent future incidents
- Identify root cause analysis
- Review of the current incident response process
- Identification of tools and resources victim could utilize for prevention
- Review of actions taken by response team, including items that identify the need for improvement to the response plan.
- Schedule tabletop exercises to practice incident response plan

State and Federal Resources Available | Locality or Third Party Responsibility | State and Federal Resources Available

UNDERSTAND

- Inventory
  - You can’t secure what you don’t know you have.
- Shield Wall
  - Build partnerships with insurance, peers, state & federal partners, and consultants
- Know your responsibilities
  - Legislation, mandates, regulations
  - What data do you have? (PCI, PII, HIPAA, FERPA, CJIS, Elections, etc.)
- Understand your risk (read as LIABILITY)
  - Do not be afraid of a risk assessment. Even a napkin assessment will help.

PREPARE (Incident Response Framework)

- Support/sponsorship from the top
- Pick a framework and measure against it
  - CIS is easiest to digest
  - NIST is commonly used for reporting to state and federal partners
- Audit…remediate…test…repeat
  - Pentest, vulnerability assessments, hygiene scans, tabletop exercises.
- Nail down your policies
- Document your preparations and Incident Response Plan
  - Communication Plan & Protocols
    - Internal stakeholders (administration, finance, legal)
    - External partners (insurance, law enforcement, state/federal entities, vendors, ISP)
    - Media (follow legal counsel's script!)
- Document procedures to support the polices and your response protocol

What sort of questions will you get?

- How do you identify there is a problem?
- What do you know about what happened?
- What networks/systems/data are affected?
- What data/information was compromised (e.g., stolen, deleted, altered)?
- When did the breach occur?
- When did you find out about it?
- When did you begin to do something about it?
- When will you know the full scope of the problem?
- When do you estimate that the problem will be remediated?
- Where did the breach occur (what office, activity, locale, etc.)?
- How much do you know, with certainty, about how the breach occurred? The source of the attack?
- How will you stay informed of efforts to remediate the breach and restore normal service?
- AND SO MANY MORE…in other words, **preparation is key to rapid and effective response.**
  - **Knowing what to expect for response will help you build your preparations to respond**

Incident Response Plan

- Define a team
- Determine roles and responsibilities
- Create internal and out-of-band communication paths
- Train all levels
- Establish Single point of contact
- Review plan regularly
- Test the plan

Suspected Cyber Incident

- **<u>Notify your insurance provider</u>**
- Implement your Incident Response Plan
- Act quickly
- Protect your data
  - Take machines off networks and information offline
  - Preserve all logs
- Document as much as possible

Suspected Cyber Incident

- You may have a **Breach Coach** based on event type
  - Determine other players to get involved
  - Assist with Public Relations
- **Make no public statement or contact third parties without consultingthe Coach**
  - Entering into an agreement with an outside provider without authority could violate the coverage contract

Cyber Breach Coach

- Skilled Attorney -Today’s Threats and Tomorrow’s Risks
- Secures Attorney Client Privilege
- Engages Necessary Third Parties
  - Law Enforcement, Forensic Firms, Public Relations
- Identifies Reporting Necessity
- Knows Specialties of Forensic Firms
- Accessible Throughout Event

Provide Information

- Main contact
- Log Information
- Name/Contact of ISP, Contract IT, and third-party email/web support
- Copy of email and/or ransom message
- Wire transfer information
- Known users on affected machine(s)
- Email: cloud-based or on site (365, Gmail, etc)

Preserve Logs

- One of the first things forensics and attorneys will ask for
- Do not let logs roll over/overwrite
- Log review is best way to confirm that constituent data is only encrypted and not exported
- Capture logs at a

QUESTIONS?

virginia
association
of planning
district commissions