Technology Incident Response and Impact Reduction

May 9, 2018

David Litton

dmlitton@vcu.edu

VCU

Incidents and Impacts

Yahoo!
EQUIFAX

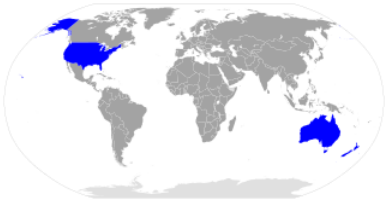
MedStar

Dyn, Inc.

- Stolen Data

- Destroyed Data

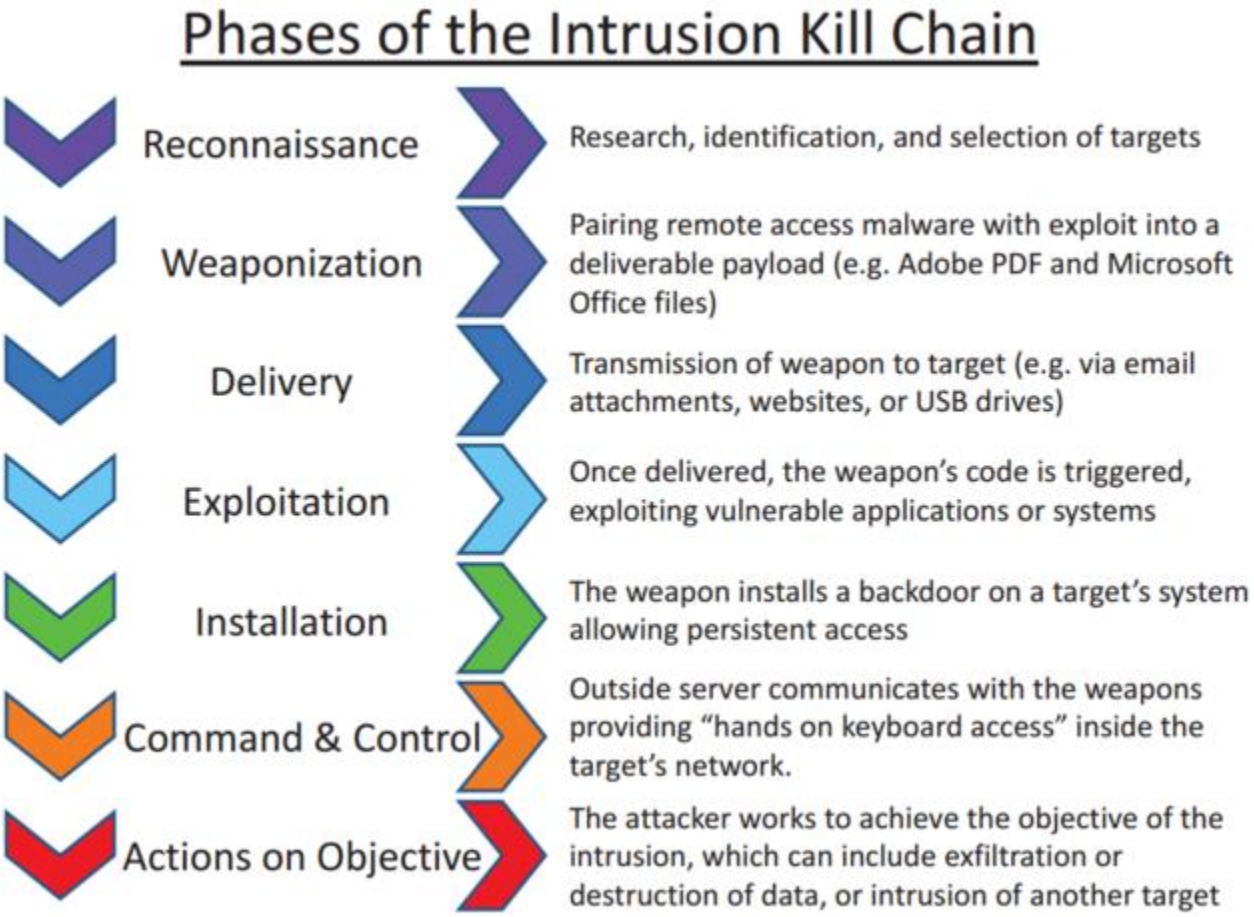
- Lost Service / Availability



- Possible Stolen Data

VCU

Intrusion / Cyber Kill Chain



Developed by Lockheed Martin, Inc.

Important Terms

- Event: any observable occurrence in a system or network
- Computer Security Incident: a violation of or imminent threat to computer security policies
- Escalation Criteria: Who to involve by when and how (Test!)
- Ransomware: a malicious software or cryptovirology threatening to publish or perpetually block access to data unless a ransom is paid
- SOC: security operations center
  - ❖ Fully Managed SOC-as-a-Service – SOC and SEIM outsourced
  - ❖ Co-managed SOC-as-a-Service – Remote SEIM monitoring
  - ❖ Hybrid or Custom – Build your own

Important Terms (continued)

- IDS: intrusion detection system (Cisco, TrendMicro, McAfee)
- IPS: intrusion prevention system (FireEye, Alert Logic, NSFOCUS)
- File Integrity Monitoring (TripWire, EventSentry, Alien Vault)
- DLP: data loss prevention (Symantec, TrustWave, Check Point)
- Virus software: definition-based detection (file hashs) (McAfee)
- Malware software: (MalwareBytes, Sophos, Webroot, Kapersky)
- Endpoint Protection: Workstation/Servers via Heuristic / Anomaly

Quick note: The importance of workstation and database encryption

Security Incident Software

- SIEM (Security Information and Event Management)
  - Security event collector and correlation tool set
    - ❖Custom / proprietary solution
    - ❖Open Source (OSSEC, SNORT, ELK, PRELUDE, OSSIM)

- SIM and SEM function together as SIEM
- SIM - Collector – gathers traditional logs then parses, aggregates, and normalizes events (e.g. Syslog and Windows)
- SEM receives events then correlates, analyses, alerts
- Examples: ArcSight, Q-Radar, LogRhythm, McAfee, Splunk

Possible Devices Connected to SIEM

- Active Directory/Domain Controllers
- Firewall
- Network routers and switches
- Network event/flow monitoring devices
- Virus software console
- Operating systems such as Unix/Linux and Windows
- Database servers
- Web servers

❑ Many use SysLog to store and spool system events

Ransomware, Malware, Spyware and How They Enter Your Organization

- Phishing/Email containing bad URLs and EXEs
- Surfing infected websites
- Poor workstation patching including Adobe Flash
- Administrative accounts on workstations (allow for remote installation of nefarious software)
- Macros (Microsoft Office/365)
- Portable storage (CDs, USB drives, etc.)
- Direct hacks against perimeter servers then used to “Worm” through the network

Phishing / Spearphishing

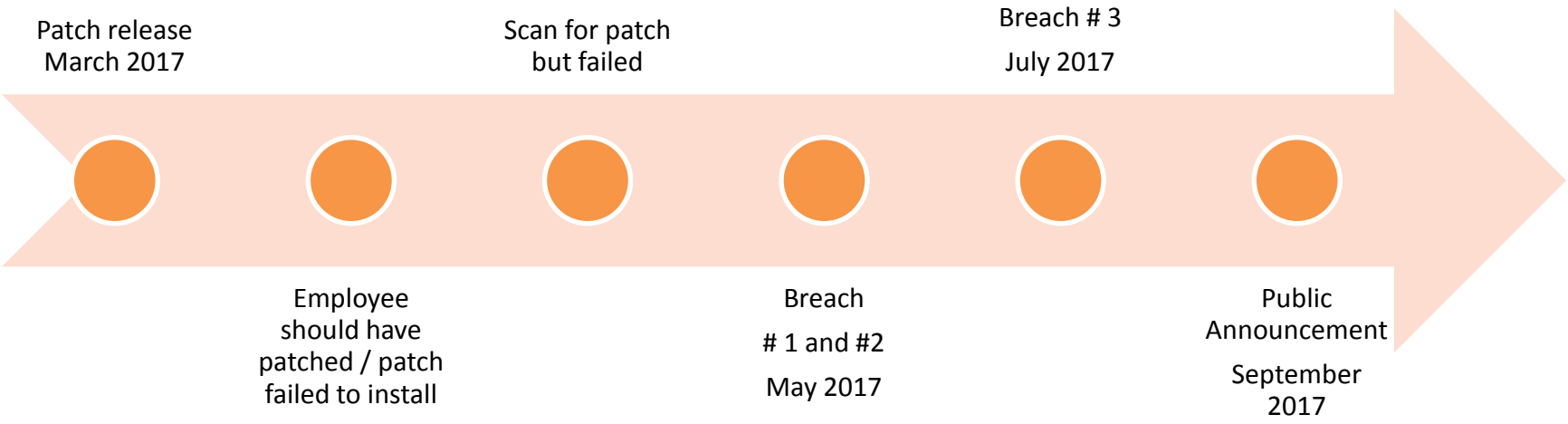
- Phishing: Access a victim's personal information through a scam email.
- Spearphishing: an individually tailored and official-looking e-mails to lure victims to fake websites or open an infected file.
- Consider administering fake phishing campaigns by ISO/IT
- VCU PhishingNet: http://phishing.vcu.edu/

- Student, faculty and staff **training** is KEY!

NIST Pub 800-61 – Computer Security Incident Handling Guide

1. Organizing a Computer Security Incident Response Capability
   - Events and incidents monitoring and identification, respectively
   - Incident response, policy, plan, and procedure creation
   - Incident response team structure
2. Handling an Incident
   - Preparation
   - Detection and analysis
   - Containment, eradication, and recovery
   - Post-incident activity
3. Coordination and Information Sharing
   - Coordination
   - Information sharing techniques
   - Granular information sharing

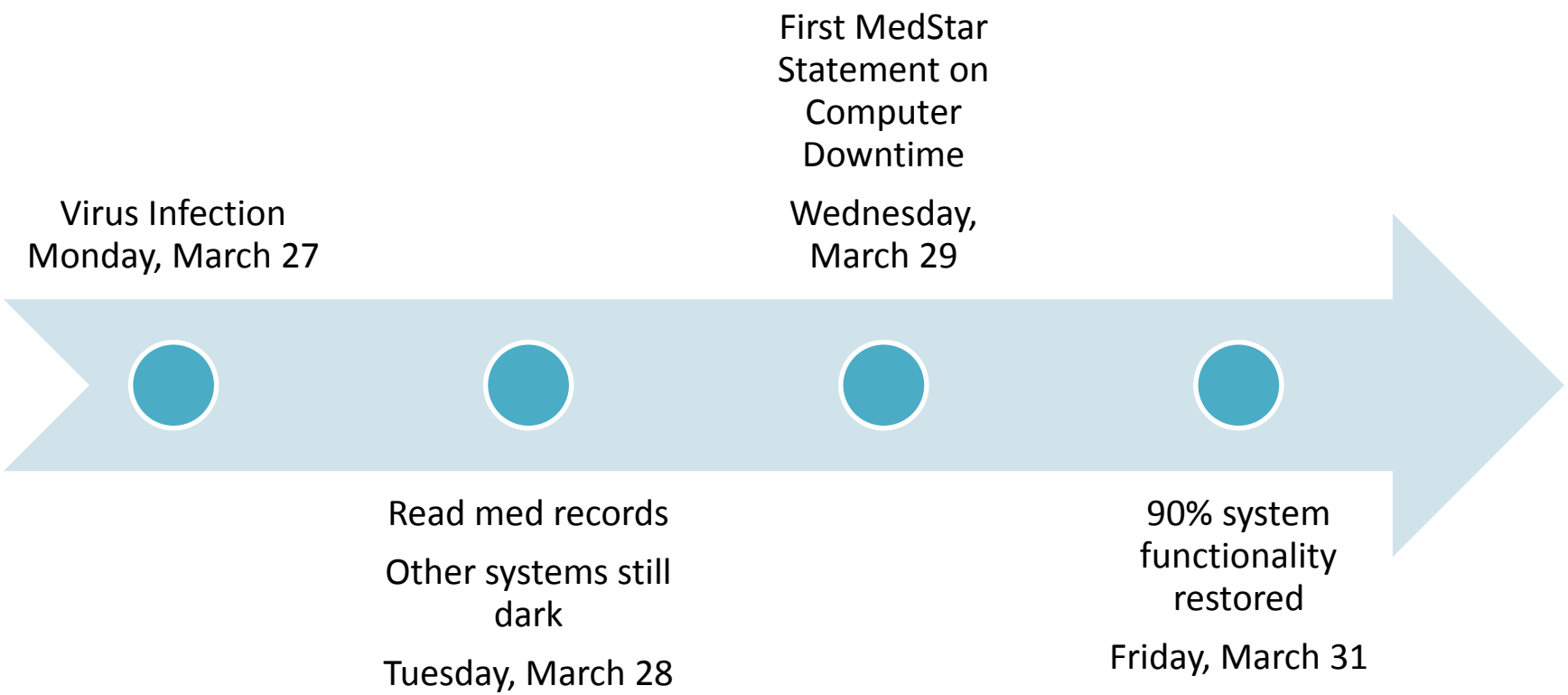
Timeline for Equifax Breach



Controls to Mitigate a Future "Equifax or VCU – like" Data Exfiltrations

1. "Database Activity Monitoring" to identify copying entire database
2. Better monitoring of network flow(s)
3. Increased network segmentation
4. Effective encryption of the database
5. Patching schedules/logs and patch verification
6. Hardened O/S configuration and remove default passwords
7. Security forensics firm (potentially on retainer)
8. Cyber insurance company involved early
9. Better customer communication (reduce Reputational Risk)

Timeline for MedStar Ransomware Breach 2016



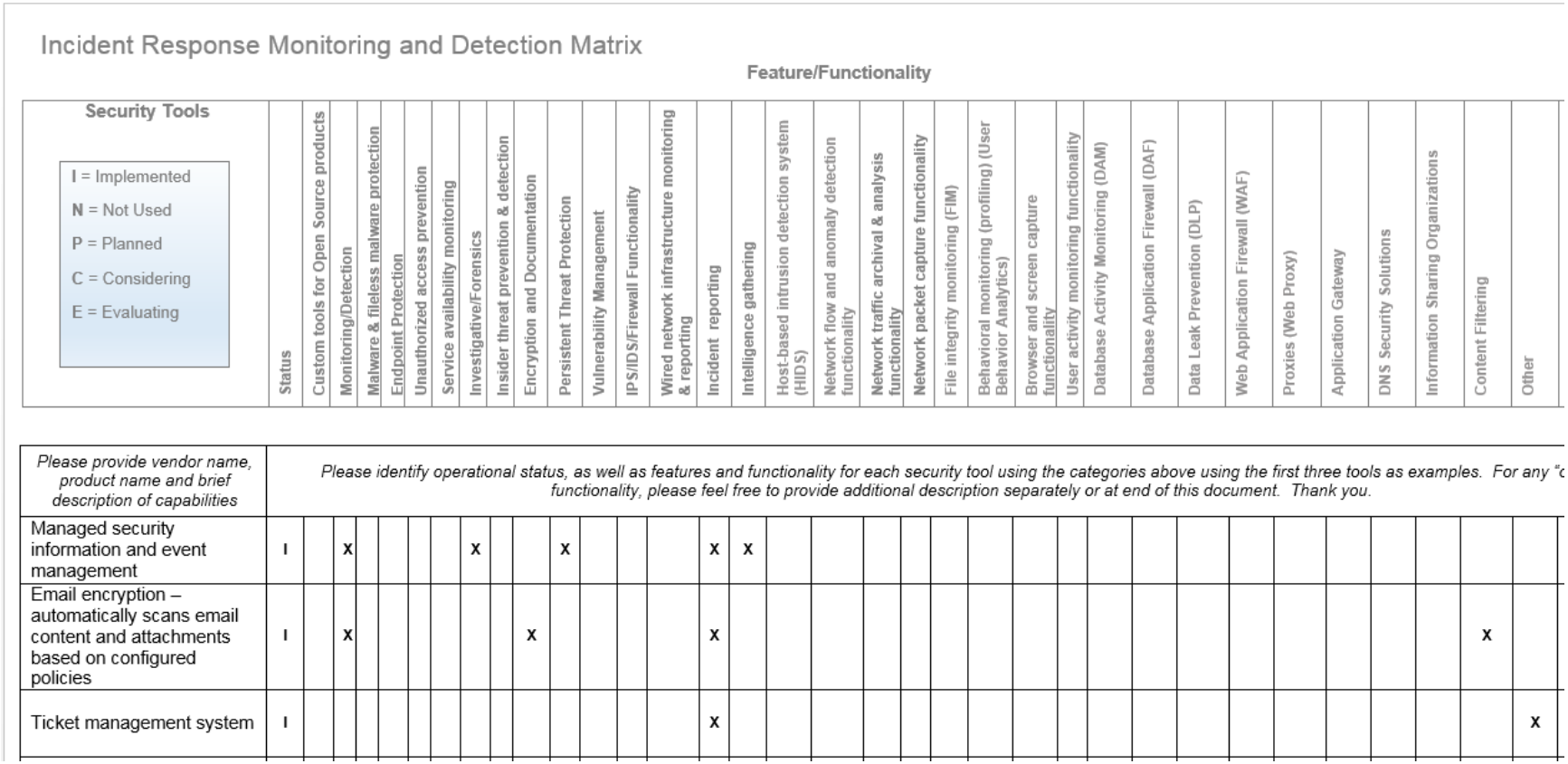
Controls to Mitigate a Future "MedStar-like" or Other Ransomware Attacks

1. Endpoint protection
2. Updated operating systems
3. Restricting old network communications protocols (SMB v1)
4. Training on phishing
5. Workstation backups or folder redirection (file share policy)
6. External drive restrictions (thumb drives, CDs)
7. Patching schedules/logs and patch verification
8. No world-writable file shares
9. Previous discussion with Board on paying / not paying

Intrusion / Cyber Kill Chain

Developed by Lockheed Martin, Inc.

IR Monitoring and Detection Software – Gap Analysis



Incident Response Monitoring and Detection Matrix

Feature/Functionality

Security Tools I = Implemented N = Not Used P = Planned C = Considering E = Evaluating	Status	Custom tools for Open Source products	Monitoring/Detection	Malware & fileless malware protection	Endpoint Protection	Unauthorized access prevention	Service availability monitoring	Investigative/Forensics	Insider threat prevention & detection	Encryption and Documentation	Persistent Threat Protection	Vulnerability Management	IPS/IDS/Firewall Functionality	Wired network infrastructure monitoring & reporting	Incident reporting	Intelligence gathering	Host-based intrusion detection system (HIDS)	Network flow and anomaly detection functionality	Network traffic archival & analysis functionality	Network packet capture functionality	File integrity monitoring (FIM)	Behavioral monitoring (profiling) (User Behavior Analytics)	Browser and screen capture functionality	User activity monitoring functionality	Database Activity Monitoring (DAM)	Database Application Firewall (DAF)	Data Leak Prevention (DLP)	Web Application Firewall (WAF)	Proxies (Web Proxy)	Application Gateway	DNS Security Solutions	Information Sharing Organizations	Content Filtering	Other
Please provide vendor name, product name and brief description of capabilities	*Please identify operational status, as well as features and functionality for each security tool using the categories above using the first three tools as examples. For any "o functionality, please feel free to provide additional description separately or at end of this document. Thank you.*																																	
Managed security information and event management	I		X					X			X				X	X																	
Email encryption – automatically scans email content and attachments based on configured policies	I		X							X					X																	X	
Ticket management system	I														X																		X

Questions and Comments