UVM Medical Center Cyber Attack

October 2020

THE University of Vermont HEALTH NETWORK

What Happened?

- Email phishing attack
- Encrypted 1300 servers – core infrastructure
- Malware on 5000 devices for persistence
- Epic not impacted directly
- No data breached

Immediate Response

Call to arms:

- Incident command
- Activated cyber security forensics retainer
- Contacted law enforcement

Red Button

- Shutdown all network systems
- Took down Epic
- Perimeter network lockdown
- BCA Mode

What Worked

- Close collaboration with law enforcement
- Make decisions, ask forgiveness
- IT incident command
  - Operational Leaders
- Hospital incident command
  - Clinical and operational leaders
  - IT leaders attended (and vice-versa)
  - Prioritized system restore
  - Made clinical care and service decisions

Challenges

- Downtime procedures
  - Only three days of data in Epic downtime computers
  - Staff rusty on procedures
- Communication
  - Phones down initially – walkie-talkies and runners
  - BYOD
  - Internal/external communication workflows
- Paper everywhere
  - Paper orders and notes
  - Thousands of lab orders and results
  - Processing and storage
- Remote workforce
  - Set-up Teams channels for key work streams
- Daily clinical service and patient safety decisions

Key Learnings

- Cyber security must be a top organizational priority
- Ensure your downtime procedures and data anticipate a potential prolonged downtime
- Response to a cyber attack requires “all hands on deck” not just IT hands
- Review your cyber insurance plans now

UVMHN Cybersecurity Program

Cybersecurity Enhancements

Enhancement	Impact
Deployed Zscaler agents to all remote and mobile workstations	Expanded UVMHN's web security filtering capabilities already in place for onsite personnel to all remote and hybrid workforce members
Implemented Zscaler's Advanced Firewall and Cloud Sandbox	Expanded internet security filtering capabilities from web to all applications and services and added the capability to inspect internet downloads in the cloud for malicious behavior
Deployed Crowdstrike NGAV & EDR	Added a Next Generation Anti-Virus and Endpoint Detection and Response agent to all workstations and servers that both helps prevent advanced malware and aids in the investigation and response to any successful cyber attack
Engaged Crowdstrike Overwatch Services	Added a 24/7/365 managed service to bolster UVMHN's Cybersecurity Operations team providing constant threat monitoring and hunting through the Crowdstrike platform
Deployed Splunk Phantom SOAR	Replaced the Security Orchestration and Automated Response platform with a new solution more tightly aligned with the UVMHN security event monitoring platform enabling stronger integrations and automation
Launched Proofpoint phishing platform	Enabled the capability to conduct internal phishing simulation campaigns with built in targeted awareness training for susceptible users

Cybersecurity Architecture

Network Security

- Zscaler Internet Access with network tunneling and remote agent deployment, SSL inspection, and cloud malware sandboxing
- Zscaler Layer 7 application firewall with IDS/IPS
- Cisco VRF & ASA based macro segmentation
- VMWare NSX Datacenter Micro Segmentation (in development)
- CISCO ISE Campus Micro Segmentation (in development)

Endpoint Security

- Crowdstrike Next Gen AV and EDR with Overwatch 24/7 managed threat hunting services
- Microsoft System Center Configuration Manager
- Citrix EMS Mobile Device Management
- Microsoft Intune Mobile Application Management

Email Security

- Microsoft Advanced Threat Protection for Exchange Online with malware sandboxing
- Proofpoint phishing simulation and cyber awareness platform
- Microsoft Data Loss Protection

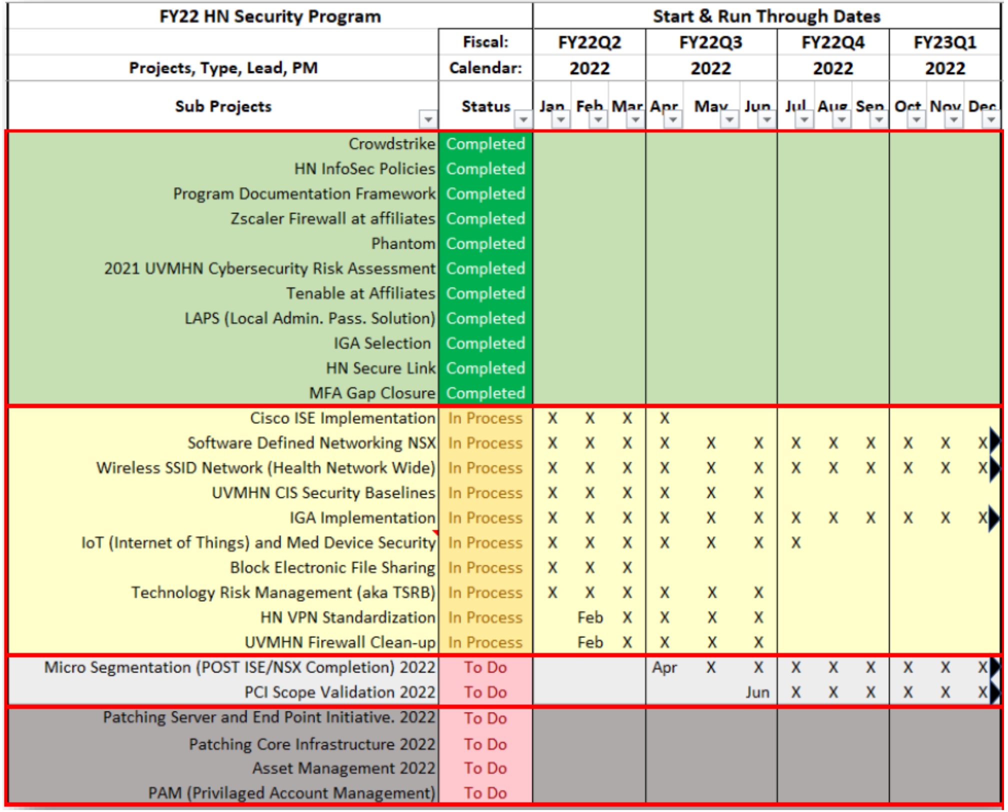
Identity and Access Management

- AzureAD and ADFS SAML based SSO
- Imprivata Enterprise SSO and badge access
- Azure MFA with Microsoft Authenticator
- Azure Conditional Access for Office 365
- SecureLink vendor access management platform
- IGA Platform Selection - Sailpoint

Monitoring and Response

- Splunk Enterprise Security SIEM
- Splunk Phantom Security Orchestration and Automated Response platform
- Tenable.IO vulnerability management platform

Information Security Program



FY22 HN Security Program		Start & Run Through Dates											
	Fiscal:	FY22Q2			FY22Q3			FY22Q4			FY23Q1		
Projects, Type, Lead, PM	Calendar:	2022			2022			2022			2022		
Sub Projects	Status	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Crowdstrike	Completed												
HN InfoSec Policies	Completed												
Program Documentation Framework	Completed												
Zscaler Firewall at affiliates	Completed												
Phantom	Completed												
2021 UVMHN Cybersecurity Risk Assessment	Completed												
Tenable at Affiliates	Completed												
LAPS (Local Admin. Pass. Solution)	Completed												
IGA Selection	Completed												
HN Secure Link	Completed												
MFA Gap Closure	Completed												
Cisco ISE Implementation	In Process	X	X	X	X								
Software Defined Networking NSX	In Process	X	X	X	X	X	X	X	X	X	X	X	X ▶
Wireless SSID Network (Health Network Wide)	In Process	X	X	X	X	X	X	X	X	X	X	X	X ▶
UVMHN CIS Security Baselines	In Process	X	X	X	X	X	X						
IGA Implementation	In Process	X	X	X	X	X	X	X	X	X	X	X	X ▶
IoT (Internet of Things) and Med Device Security	In Process	X	X	X	X	X	X	X					
Block Electronic File Sharing	In Process	X	X	X									
Technology Risk Management (aka TSRB)	In Process	X	X	X	X	X	X						
HN VPN Standardization	In Process		Feb	X	X	X	X						
UVMHN Firewall Clean-up	In Process		Feb	X	X	X	X						
Micro Segmentation (POST ISE/NSX Completion) 2022	To Do				Apr	X	X	X	X	X	X	X	X ▶
PCI Scope Validation 2022	To Do						Jun	X	X	X	X	X	X ▶
Patching Server and End Point Initiative. 2022	To Do												
Patching Core Infrastructure 2022	To Do												
Asset Management 2022	To Do												
PAM (Privilaged Account Management)	To Do												