Joshua Marzan Daniel Rivera Group 5 Capstone

Key points to consider:

- What is the backstory of PMC?
  There was a cybersecurity attack initiated by a user clicking a malicious email link, which injected a payload into some devices, eventually opening up a vulnerability leading into a ransomware attack. We were hired not only to improve on the day to day network efficiency, but to ensure a more secure network and implement user training. Any chain is as strong as its weakest link, so we are attempting to strengthen any area that might lead to a compromised vulnerability.

- What changes did we make?
  We decommissioned previous network equipment, installed some new networking equipment, along with implementing security measures to meet our HIPAA regulations. New network + secure. Adding 3rd party cyber security services to outsource things like monitoring (RocketCyber), endpoint protection (SentinelOne), user cybersecurity training (KnowBe4), and email security (Mimecast).

- Site to site VPN? What is it and who is supporting our site to site VPN?
  A site-to-site virtual private network (VPN) is a connection between two or more networks, such as a corporate network and a branch office network. Many organizations use site-to-site VPNs to leverage an internet connection for private traffic. Implemented through Fortigate and active/passive redundancy for the firewalls; Dual internet connection capabilities. We have two ISPs, for the network completely both would have been down which is unlikely.

- How are AT&T and Comcast supporting our network?
  AT&T Dedicated Business Ethernet and Comcast Business Ethernet - our data rate is 10Gb at each building to accommodate for the services we are hosting like telemedicine, EHR traffic flow, and daily activities that come with providing efficient healthcare patients.

- What are some of our update procedures whilst maintaining five nines (99.999%) availability?
  Rolling updates, virtual environment setup for testing, maintenance windows; ServiceNow CHG management system.

- What cable are we using and how are we running it throughout our buildings?
  Cat6a STP to account for any EMI that may be present in the environment and we are running through PVC pipes and plenum spacing (ceilings, floor).

- How are we subnetting? What are our subnets (CIDR notation)?
  Combination of /22, /26 /27, /29 networks across all four buildings. 192.168.0.0/16 is the private IP address space we are utilizing.

- ACLs (note for me: write some ACLs) - what kind of traffic is allowed?
  We are disabling RDP traffic, TeamViewer traffic into our network. Using RDP within the network is acceptable, but we don't want other users to be able to remote into devices from outside our network.

- What security measures are we taking physically and logically? Encryption methods, email security?
  Our FortiGate firewall will encrypt the data in transit (AES-256). Data at-rest will be encrypted with volume encryption via Bitlocker Encryption (which is already included in our current Windows license). Email security will be handled through Mimecast. Where we can set rules based on domains that are coming in, attachments that will be blocked, spam policies, impersonation detection, etc. WPA3-Enterprise on the wireless side - WPA3-Enterprise builds upon the foundation of WPA2-Enterprise with the additional requirement of using Protected Management Frames on all WPA3 connections. For users logging in via VPN, have Microsoft MFA setup through Microsoft Azure.

- How are we securing IoMT devices?
  Placing IoMT devices in its own VLAN separates it from the main network traffic. If a vulnerability is found and used in the VLAN, it will be isolated from the main network. If possible, update the software for IoMT devices.

- How are we monitoring user activity in the EHR space? How are we doing audits?
  Windows Server has an auditing function that can be enabled. Active Directory also logs user login information and times as well.

- User training? How is it conducted?
  Specific user training regarding the handling of data under HIPAA compliance is conducted through the HIPAA Compliance Officer that will be hired. Basic cybersecurity training will be implemented through KnowBe4, which has video modules and questions for users to complete. In addition, it sends fake "phishing"

emails using fake internal email addresses and names of employees, to simulate phishing attempts from actual threats.

Labor cost: 9 workers making $35/hour (8 hour workdays for a year) = $72,800 * 9 workers = 655,200 + year 1 cost = $7.9 million

- SVIs take the first IP address of the VLANs to give the VLANs a gateway to route traffic

Sample config:
OSPF (backbone area configs)

```
MultiSwitch1(config)# router ospf 1   # Enter OSPF configuration
mode with process ID 1
MultiSwitch1(config-router)# network 192.168.32.0 0.0.0.63 area 0
MultiSwitch1(config-router)# network 192.168.35.0 0.0.0.31 area 0
MultiSwitch1(config-router)# network 192.168.37.0 0.0.0.31 area 0
MultiSwitch1(config-router)# network 192.168.38.0 0.0.3.255 area 0
MultiSwitch1(config-router)# network 192.168.42.0 0.0.0.63 area 0

MultiSwitch2(config)# router ospf 1   # Enter OSPF configuration
mode with process ID 1
MultiSwitch2(config-router)# network 192.168.43.0 0.0.0.7 area 0
MultiSwitch2(config-router)# network 192.168.43.8 0.0.0.31 area 0
MultiSwitch2(config-router)# network 192.168.45.0 0.0.3.255 area 0
MultiSwitch2(config-router)# network 192.168.49.0 0.0.0.7 area 0
MultiSwitch2(config-router)# network 192.168.49.8 0.0.0.31 area 0
MultiSwitch2(config-router)# network 192.168.50.0 0.0.0.255 area 0

ACLs
access-list 101 permit tcp 192.168.32.0 0.0.0.63 any eq 443
access-list 101 permit tcp 192.168.35.0 0.0.0.31 any eq 443
access-list 101 permit tcp 192.168.37.0 0.0.0.31 any eq 443
access-list 101 permit tcp 192.168.38.0 0.0.3.255 any eq 443
access-list 101 permit tcp 192.168.42.0 0.0.0.63 any eq 443
access-list 101 permit tcp 192.168.43.0 0.0.0.7 any eq 443
access-list 101 permit tcp 192.168.43.8 0.0.0.31 any eq 443
access-list 101 permit tcp 192.168.45.0 0.0.3.255 any eq 443
access-list 101 permit tcp 192.168.49.0 0.0.0.7 any eq 443
access-list 101 permit tcp 192.168.49.8 0.0.0.31 any eq 443
access-list 101 permit tcp 192.168.50.0 0.0.0.255 any eq 443

access-list 101 permit tcp 192.168.32.0 0.0.0.63 any eq 80
access-list 101 permit tcp 192.168.35.0 0.0.0.31 any eq 80
access-list 101 permit tcp 192.168.37.0 0.0.0.31 any eq 80
access-list 101 permit tcp 192.168.38.0 0.0.3.255 any eq 80
```

```
access-list 101 permit tcp 192.168.42.0 0.0.0.63 any eq 80
access-list 101 permit tcp 192.168.43.0 0.0.0.7 any eq 80
access-list 101 permit tcp 192.168.43.8 0.0.0.31 any eq 80
access-list 101 permit tcp 192.168.45.0 0.0.3.255 any eq 80
access-list 101 permit tcp 192.168.49.0 0.0.0.7 any eq 80
access-list 101 permit tcp 192.168.49.8 0.0.0.31 any eq 80
access-list 101 permit tcp 192.168.50.0 0.0.0.255 any eq 80
```

```
Configure ACL to allow email traffic (SMTP - TCP Port 25 and IMAP -
TCP Port 143)
access-list 101 permit tcp 192.168.32.0 0.0.0.63 any eq 25
access-list 101 permit tcp 192.168.35.0 0.0.0.31 any eq 25
access-list 101 permit tcp 192.168.37.0 0.0.0.31 any eq 25
access-list 101 permit tcp 192.168.38.0 0.0.3.255 any eq 25
access-list 101 permit tcp 192.168.42.0 0.0.0.63 any eq 25
access-list 101 permit tcp 192.168.43.0 0.0.0.7 any eq 25
access-list 101 permit tcp 192.168.43.8 0.0.0.31 any eq 25
access-list 101 permit tcp 192.168.45.0 0.0.3.255 any eq 25
access-list 101 permit tcp 192.168.49.0 0.0.0.7 any eq 25
access-list 101 permit tcp 192.168.49.8 0.0.0.31 any eq 25
access-list 101 permit tcp 192.168.50.0 0.0.0.255 any eq 25
access-list 101 permit tcp 192.168.32.0 0.0.0.63 any eq 143
access-list 101 permit tcp 192.168.35.0 0.0.0.31 any eq 143
access-list 101 permit tcp 192.168.37.0 0.0.0.31 any eq 143
access-list 101 permit tcp 192.168.38.0 0.0.3.255 any eq 143
access-list 101 permit tcp 192.168.42.0 0.0.0.63 any eq 143
access-list 101 permit tcp 192.168.43.0 0.0.0.7 any eq 143
access-list 101 permit tcp 192.168.43.8 0.0.0.31 any eq 143
access-list 101 permit tcp 192.168.45.0 0.0.3.255 any eq 143
access-list 101 permit tcp 192.168.49.0 0.0.0.7 any eq 143
access-list 101 permit tcp 192.168.49.8 0.0.0.31 any eq 143
access-list 101 permit tcp 192.168.50.0 0.0.0.255 any eq 143
```

Router 1 (building 1) IP address: 192.168.3.1-2
Router 2 (building 2) IP address: 192.168.5.1-2
Router 3 (building 3) IP address: 192.168.7.1-2
Router 4 (building 4) IP address: 192.168.9.1-2