Cyber Security

September 5, 2019

Daniel J. Nash, MBA, PMP
Chief Information Officer
dnash@EmanateHealth.org

Prepare for When, Not If…

Cyber Breach
Lessons Learned

EmanateHealth™

Queen of the Valley Hospital

West Covina

Inter-Community Hospital

Covina

Foothill Presbyterian Hospital

Glendora

Facebook: @EmanateHealthNow
Twitter: @EmanateHealth
LinkedIn: Emanate Health

www.emanatehealth.org

Emanate Health™

3 Hospitals
1 Home Care
1 Hospice
700 Volunteers
1,000 Physicians
3,500 Employees

Hospital
Emergency Care
Home Care
Hospice
Imaging
Physician Network
Surgery Centers

National Landscape

Cyberattacks: High Frequency, Devastating Impacts, and Fast Evolution

UConn Health notifies up to 326,000 patients of data breach

Mackenzie Garrity - 22 hours ago Print | Email

SHARE

Farmington-based University of Connecticut Health sent letters to up to 326,000 patients notifying them of a recent data security incident.

Patient medical records sell for $1K on dark web

Mackenzie Garrity - Wednesday, February 20th, 2019 Print | Email

SHARE

Healthcare data protection company Protenus revealed there were 222 hacking incidents in 2018, up nearly 25 percent from 2017. Of these data breaches, more than 11 million patient records were affected, *CBS News* reports.

Often these patient records can be found on the dark web or black market. Sellers offering patient records promote

OCR investigating Banner Health for 2016 breach of 3.7 million patient records

The Arizona health system is cooperating with the investigation but expects to receive negative findings and a potential fine.

By Jessica Davis | March 21, 2018 | 12:34 PM

Update: Ransomware attack on Cass Regional shuts down EHR

Emergency and stroke patients are still being diverted to ensure patients receive the best possible care, but the Missouri health system remains fully operational thanks to its prepared incident response plan.

By Jessica Davis | July 11, 2018 | 03:21 PM

UnityPoint breaches 1.4M patient's personal information after phishing attack

Julie Spitzer - Tuesday, July 31st, 2018 Print | Email

SHARE

UnityPoint Health in West Des Moines, Iowa, notified 1.4 million patients that some of their personal information may have been compromised after hackers broke into its email system using phishing tactics, the *Des Moines Register* reports.

WHEN CYBERATTACKS HIT, DISASTER RECOVERY IS NOT ENOUGH

AUTHORED BY: BECKER'S HEALTHCARE

UNDERWRITTEN BY: IRON MOUNTAIN®

EmanateHealth

National Landscape

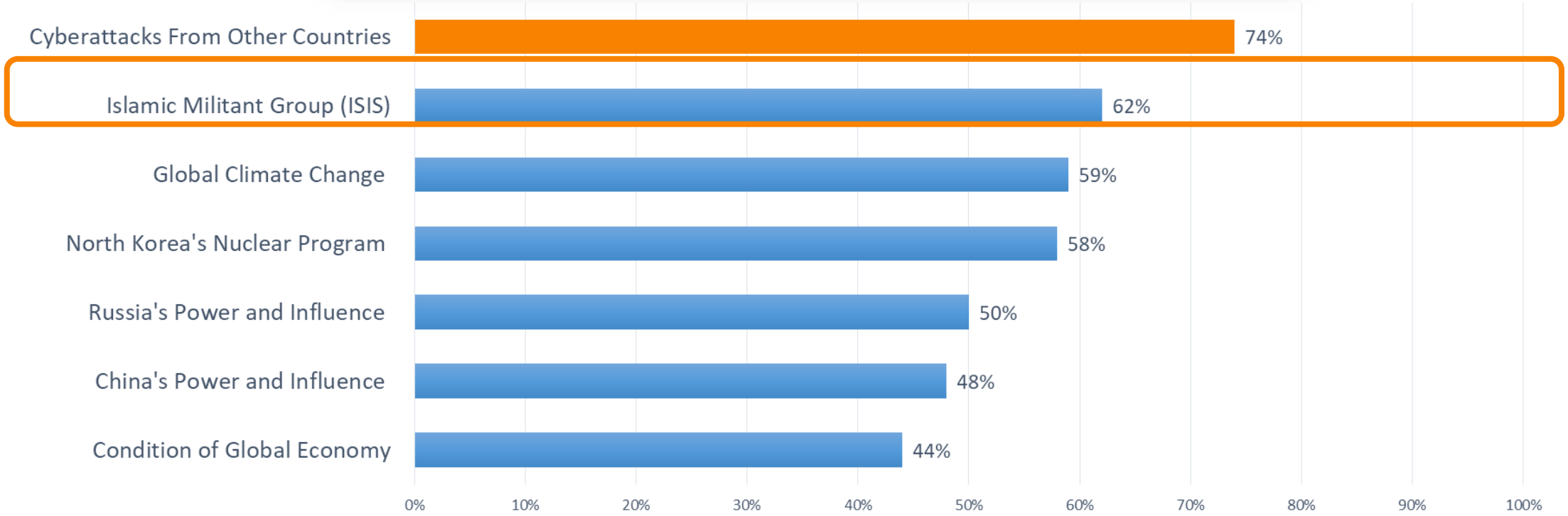
High Frequency of Perceived and Actual Cyberattacks

More Americans cite cyberattacks as more of a global threat than ISIS, climate change

Julie Spitzer - Tuesday, February 12th, 2019 Print | Email

SHARE

A cyberattack from another country is Americans' most common security concern, according to a recent survey from the Pew Research Center.



EmanateHealth

Based on data from Pew Research Center

National Landscape

Most Targeted but Underprepared for Cyberattacks: Healthcare Organizations

"In 2016, the Institute for Critical Infrastructure Technology declared healthcare as the most targeted yet underprepared sector within the United States' critical infrastructures"

Facts

40% of Healthcare Organizations have experienced a ransomware attack

69% of healthcare organizations believe their data protection infrastructure is inadequate to recover from attacks

$5M Potential Costs of Healthcare Breaches: $4M Reputational; $1M Remediation

Risk Factors

88% of IT security budgets remained level since FY 2016 in the face of increasing cyberattacks

66% of healthcare organizations have not developed a cyber incident response plan

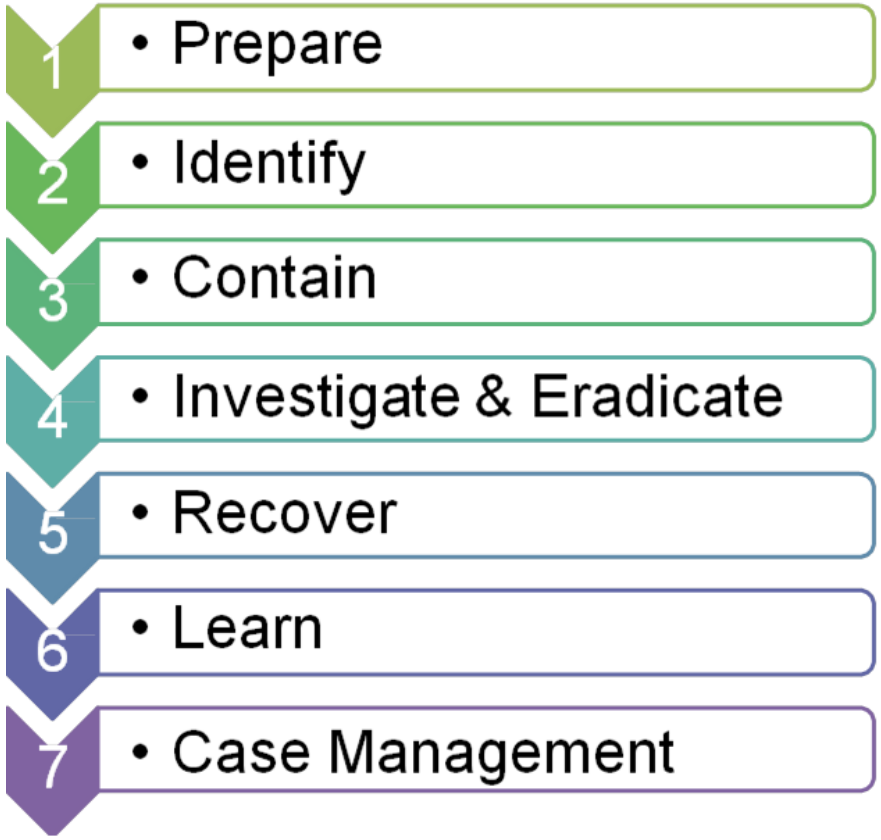
50% of healthcare organizations have cyber insurance *(Of those with no cyber insurance, 15% have no plans to purchase insurance)*

EmanateHealth

Source: Becker's Hospital Review and Iron Mountain
Source for response plan and insurance: HealthITSecurity

Response Plan

Fully Operational Cybersecurity Incident Response Plan Allows for Rapid Response During Incidents



IDENTIFY

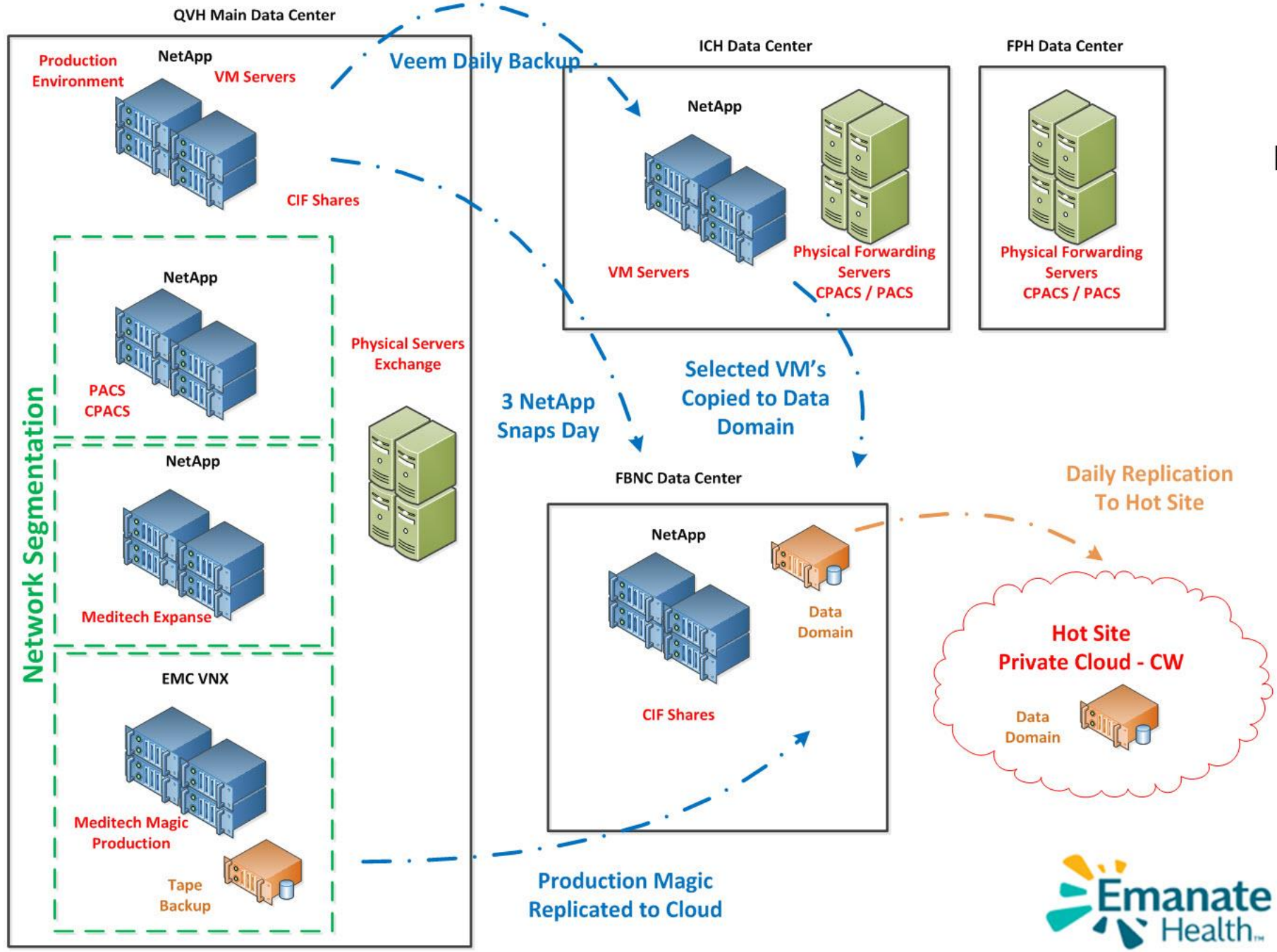
- Determine whether an incident has occurred
- Conduct an initial assessment
- Convene the IT Team
- Activate the IMT, if escalation is necessary
- Activate the CMT, if escalation is necessary
- Coordinate with third party providers
- Establish chain of custody
- Notify law enforcement, regulatory agencies, insurance company, forensic specialists, public relations firms, and credit card agencies, as appropriate

CONTAIN

- Deploy the IT Team and outside help, if necessary
- Contain the crime scene – deploy stop loss procedures
- Maintain standard response procedures
- DON'T CHANGE ANYTHING without proper authorization
- Avoid alerting the perpetrator
- Image the affected systems
- Assess the risks to continued operation
- Provide regular updates to IT, IMT, and CMT
- Change passwords for individuals/groups with access to affected system
- Staff communication – don't tell employees about incident? Just say downtime?

EmanateHealth

Computing Resources Emanate Health on 1/26/19

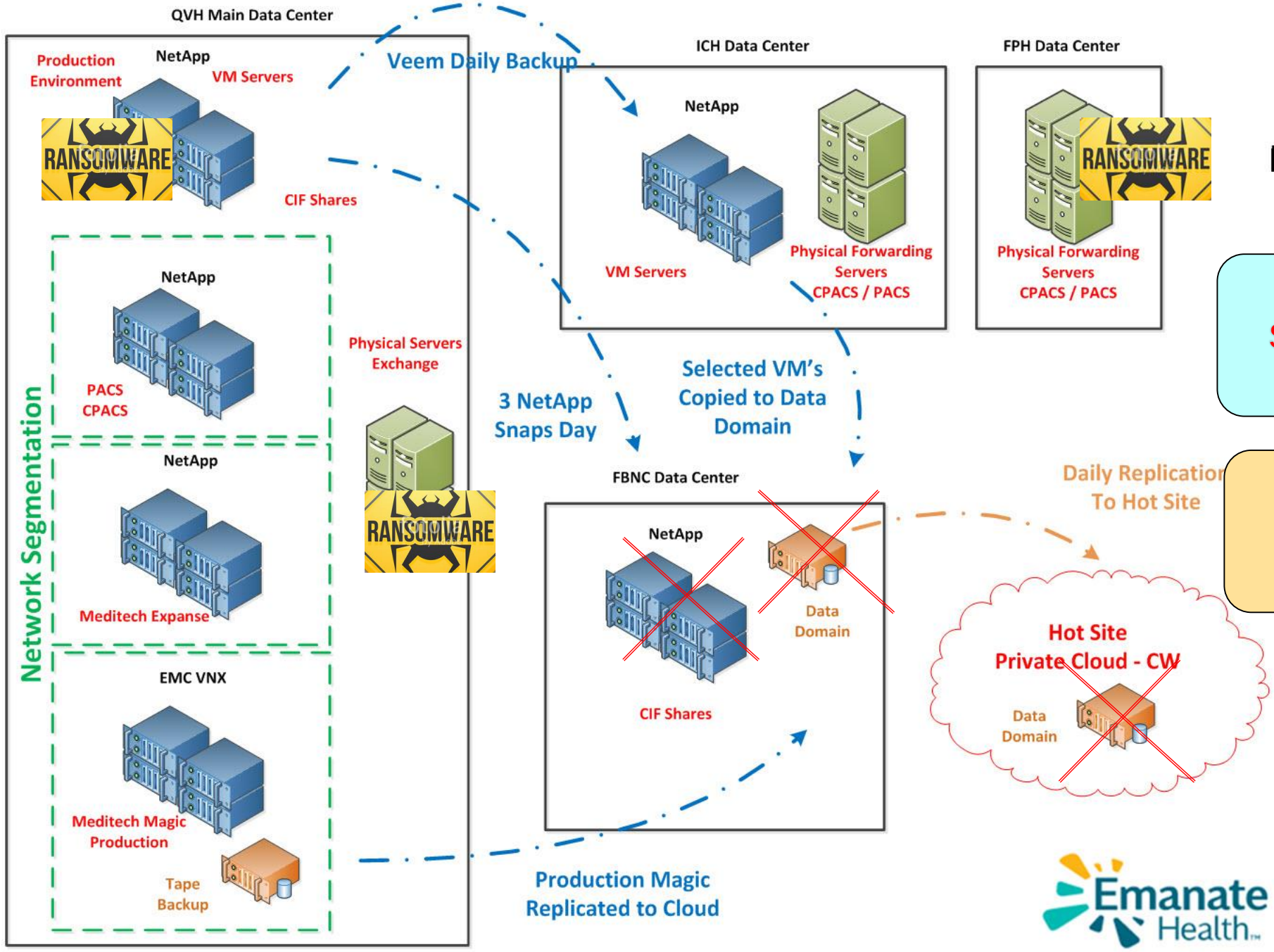


Cybersecurity Event

Minimization of Effects Due to Constant Vigilance

Cyber Breach Impacted Systems	Cyber Breach Failed to Impact
151 Servers out of 492 Servers • Archival Backup Systems • Email Exchange System • Centricity Perinatal System • Scanning & Archive OnBase • 3rd Party EHR "Bolt-on" Systems	Our Ability to See Patients Clinical Information Systems – Magic *(current EHR)* and Expanse *(future EHR)* Financial Systems Accounts Receivable System Picture Archiving and Communication System (PACS) Employee Protected and Personal Information Payroll and Timekeeping System (Kronos)

EmanateHealth



Computing Resources Emanate Health on 1/26/19

A Very Sophisticated Attack

Disabled Trend Micro Services

Emanate Health

Cybersecurity Event

Rapid Response, Robust Disaster Recovery Plan, and Foresight Prevented Potential Devastation

Hackers breached our system and were stopped soon after due to fast response time, disaster recovery plan developed in 2017, and engagement of cybersecurity law firm, cyber-forensics team, and restoration efforts

Saturday, January 26, 2019

- 02:10 am: Ransomware Detected
- 02:15 am: Incident Response Activated
- 04:20 am: Network/Systems Down
- 04:23 am: Disaster Site Put on Alert
- 04:30 am: Executive Team Updated
- 05:00 am Activate Command Center
- 05:00 am Print Downtime Reports
- Assess all Systems
- 07:00pm MEDITECH, PACS, Kronos – UP
- 11:20pm Internal Network Restored

Sunday, January 27, 2019

- 7:00 am: Review Response
- 8:00am Command Center Open
- Review & Clean Systems

Monday, January 28, 2019

- 7:00am Command Center Open
- 8:00am Review Status with E-Team
- Activate Insurance
- Engaged cybersecurity experts
  - Cybersecurity counsel
  - Cyber-forensics team
- Initiated reparation and restoration

EmanateHealth

Response

Insurance Mitigated Any Losses

Due to increasing cybersecurity attacks globally, our budget accounted for increased funds for cybersecurity protection year after year. We purchased cybersecurity insurance as a preemptive measure in June 2015.


AIG

National Union Fire Insurance Company of Pittsburgh, Pa. ®
A capital stock company

Specialty Risk Protector®

Key Elements

- Duration: 1 Year
  - 7/1/2018 – 7/1/2019
- Limit: $7.5 Million
- Premium: $87,000
- Re-Insurance: $37.5 Million
- Retention: $250,000

Coverage

- Media Content Insurance
- Security and Privacy Liability Insurance
  - Regulatory Action Sublimit of Liability
- Network Interruption Insurance
  - Waiting Hours Period (12 hours)
- Event Management Insurance
- Cyber Extortion Insurance

AIG's Role

- AIG to cover any losses
- Collaborated with cybersecurity counsel
- Assisted us with data decryption and restoration
- Engaged pre-screened experts, attorneys, and forensics team

EmanateHealth

Response

Implementation of Security Measures – In First Two Weeks After Attack

- Moved Electronic Health Record to private Cloud
- Implemented Managed Security Services – Fortigate Firewall Monitoring: live-person monitoring 24/7, 365 days per year
- Added additional Fortigate Security Tools – Firewall Web Application Filters
- Trend Micro Encryption across all machines and devices
- Implemented additional security measures on Mimecast Email Gateway

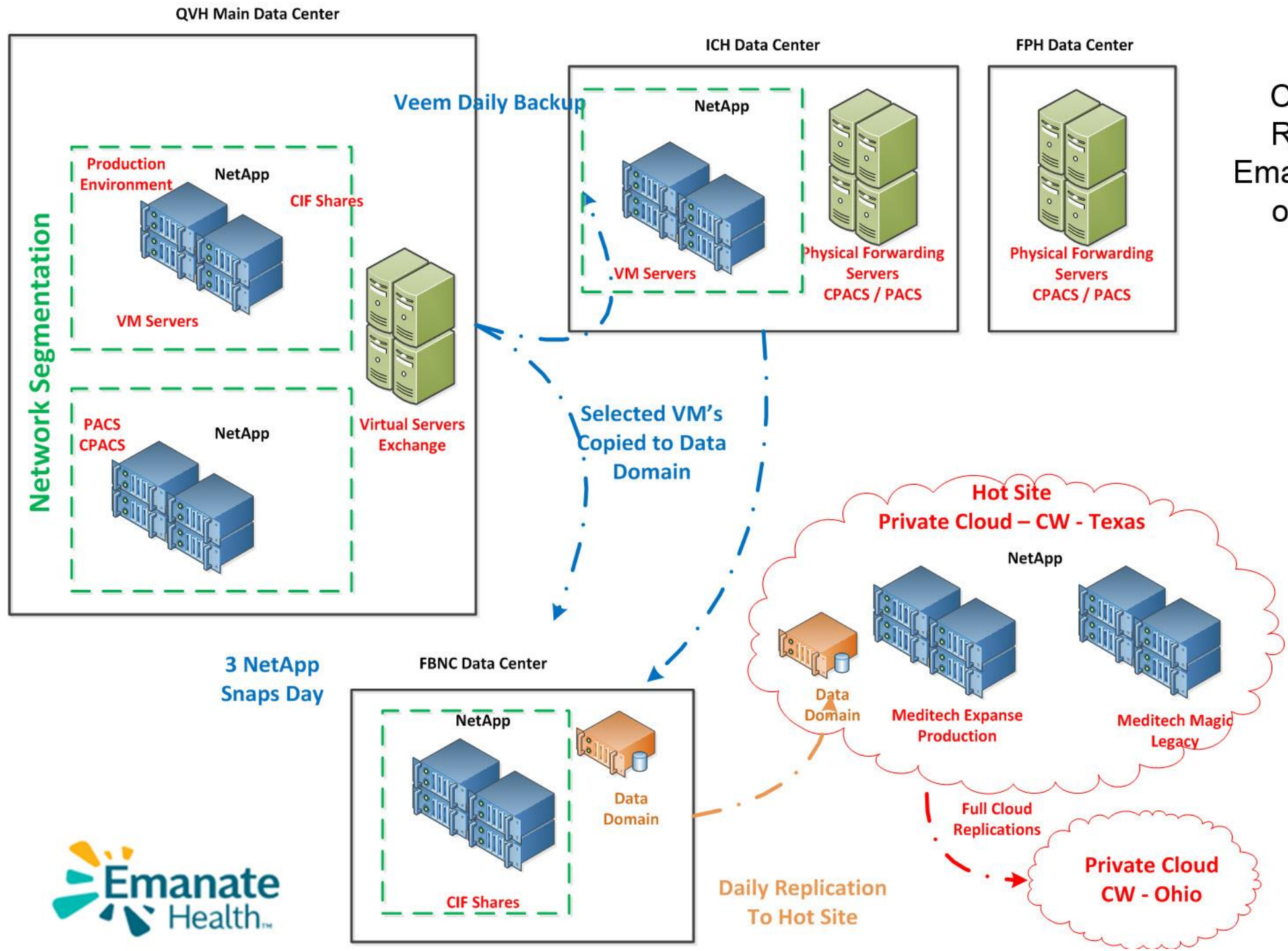
OpSus Cloud Care

FortiGate Network Security Platforms & Appliances

TREND MICRO

mimecast making email safer for business

EmanateHealth



Computing Resources Emanate Health on 2/26/19

Emanate Health

Cyber Response Results

Implementation of Security Measures

- Forensics Review and Audit – No Breach of PHI Data
  - Commended Emanate Organization on the thoroughness of documentation and responsiveness provided
  - System was penetrated using stolen credentials – “Island Hopping”
- Proposed mandate of anti-virus protection in all outside physician offices with access to our system
- Implementing two factor – authentication across all remote users
- Reducing footprint of products in DMZ for Web Facing Access
- Implementing disconnected backup strategy

EmanateHealth

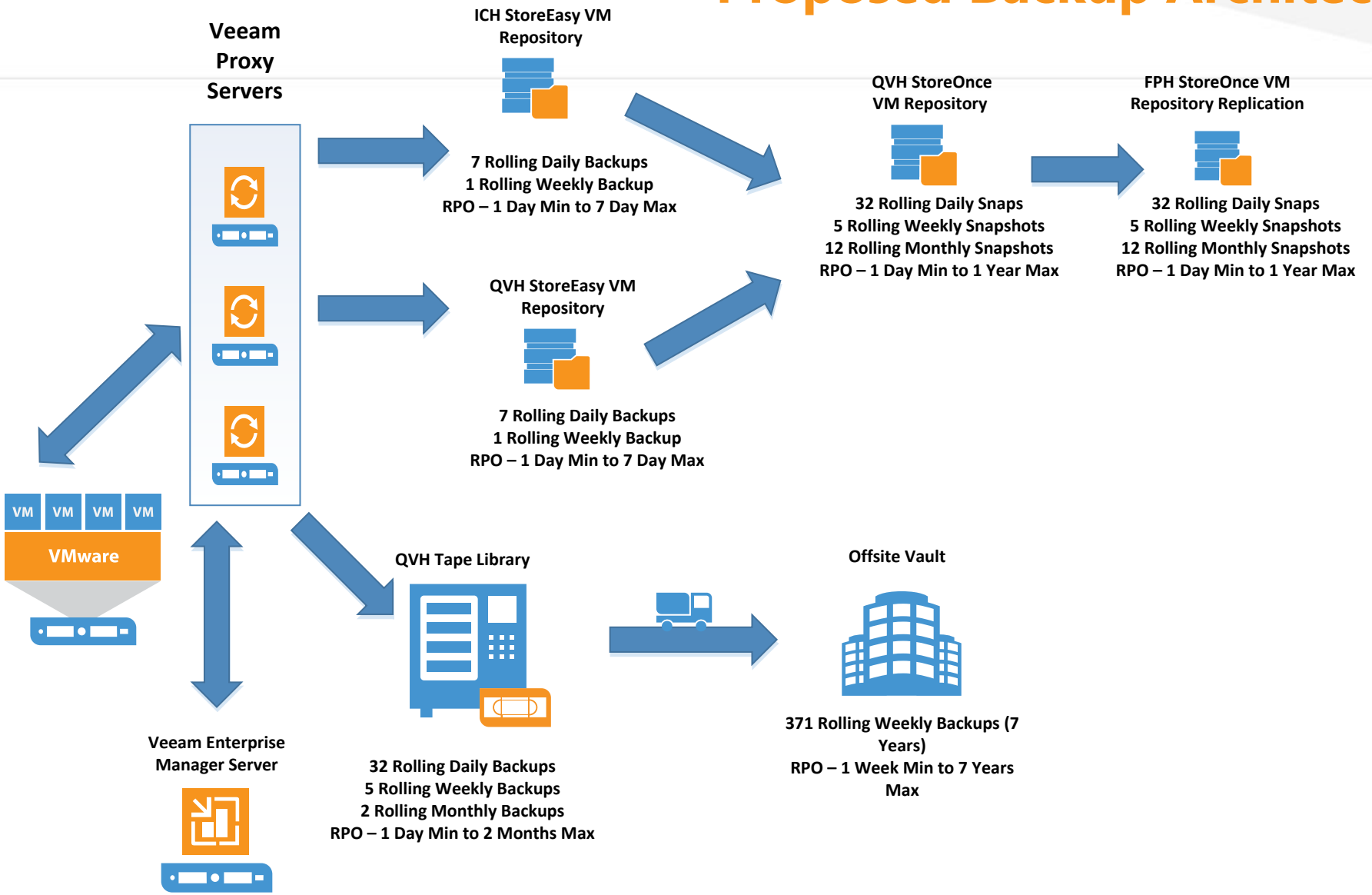
Cyber Response Lessons Learned

Implementation of Security Measures

- Downtime documentation for staff needs to be more robust
- Disconnected backup strategies
- Physical verses virtual machines
- Encryption of data at rest for all PHI/PII
- Improve alert monitoring of events – password updates, firewall traffic monitoring
- System dependency mapping
- Communication strategies – for organizational updates during event

EmanateHealth

Proposed Backup Architecture



Commendation

We continue to commend our employees and physicians for their dedication and efforts.

Key Takeaways

A Strong Organization with Engaged Staff and Physicians Dedicated to Living Our Mission

Lessons Learned

We are part of a strong organization.

TEAMWORK RESOLVE INNOVATION

ACCOMODATION COMPASSION COMMUNICATION

Our Mission

Under threat, we continued living our mission in every moment.

To help people keep well in body, mind and spirit by providing quality health care services in a safe, compassionate environment.