HHS 405(d)
Aligning Health Care
Industry Security Approaches

Healthcare & Public Health
Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

Healthcare Cybersecurity: Stay One Step Ahead of the Hackers

Ram Ramadoss, System SVP – Privacy and Information Security, CommonSpirit Health
Ido Geffen, VP Product & Customer Success, CyberMDX

Message from the 405(d) Team

The 405(d) Aligning Health Care Industry Security Practices initiative, along with the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication and this engagement, are in partnership with the Healthcare & Public Health Sector Coordinating Council (HSCC).

Healthcare & Public Health Sector Coordinating Council
PUBLIC PRIVATE PARTNERSHIP

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) Task Group member; each iteration does not reflect the views of HHS as a whole. All Task Group Members have been invited to contribute this webinar series.

* This Webinar is being recorded and will be available for future viewing

405(d) Events and Announcements

- June
  - 405(d) Spring Campaign Continues! This month's theme: "Evolution in Cybersecurity"
- July
  - 405(d) Post Volume VI to be released 7/16
  - Checkout our Social Media Awareness campaigns at @ask 405(d) on Twitter Facebook and Instagram!
- August
  - 405(d) Spotlight Webinar: Date and Topic to be announced next Month!

Today’s speakers

CommonSpirit

Ram Ramadoss

- System Senior Vice President, Privacy, Information Security and EHR Compliance
- Served as the Executive Vice President for the ISACA Denver Chapter
- Served as a core team member of the National Health Care Industry Cybersecurity Task Force
- Served as a core team member of HIMSS National Information Privacy and Security Committee
- Executive MBA - University of Michigan
- CISSP, CISA,CIPP, CISM, CRISC

CYBER MDX

Ido Geffen

- VP Product & Customer Success
- Cybersecurity Act of 2015 Section 405(d) Task Group Member
- >10 years Cyber Operations - Israeli Security Agency
- Paramedic - special combat engineering unit (5528) – Israel Defense Forces
- BSc Computer Science – Ben Gurion University & MBA – Tel Aviv University

Agenda

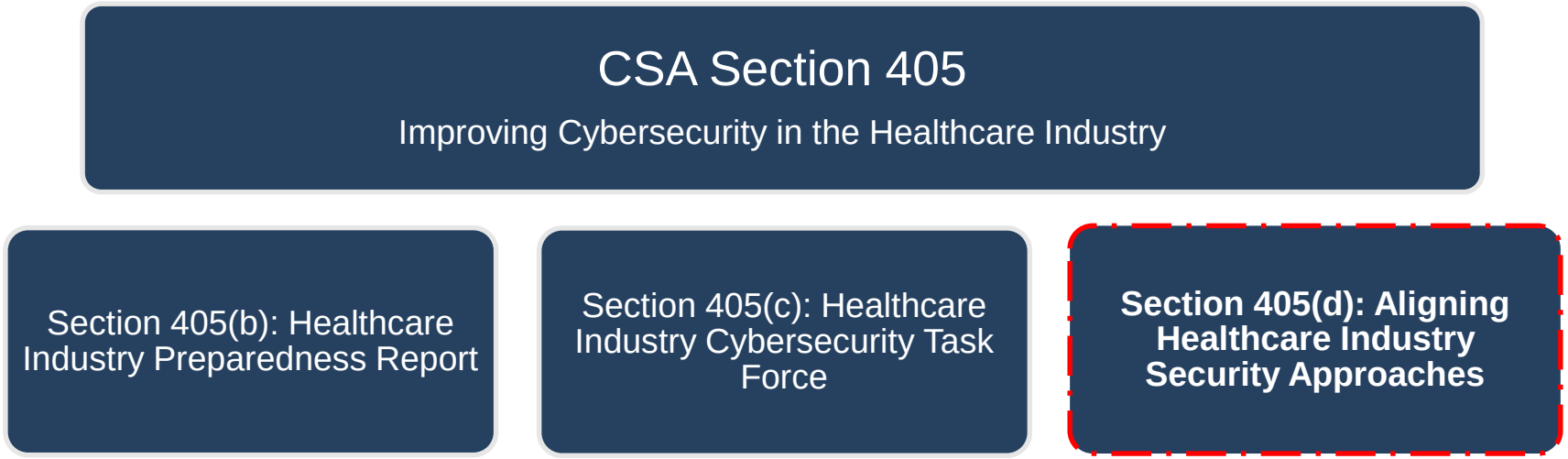
Time	Topic	Speaker
5 minutes	Opening Remarks and Introductions	Julie Chua and 405(d) Team
30 minutes	Existing and emerging cybersecurity threats to healthcare delivery organizations	Ido
20 minutes	Key challenges in balancing the resources with digital transformation and cyber resiliency	Ram
20 minutes	Brainstorm - practical recommendations and best practices (People | Process | Technology)	All
10 minutes	Communication strategies to the leadership - threats, vulnerabilities, and organization's preparedness	Ram & Ido
5 minutes	Closing	Julie Chua and 405(d) Team

Cybersecurity Act of 2015 (CSA): Legislative Basis

Under the auspices of the Cybersecurity Act of 2015 (CSA), Section 405(d), the U.S. Department of Health and Human Services (HHS) convened the CSA 405(d) public/private task group to enhance cybersecurity and align industry security practices.

The purpose of the 405(d) Spotlight Webinar is to continue the 405(d) mission and vision of “Aligning Health Industry Security Approaches” by discussing a common set of voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations.

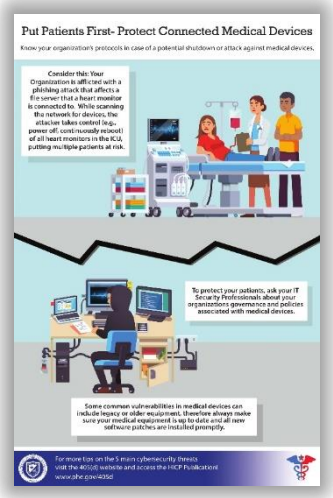
This webinar series aims to align industry security practices by providing an information sharing platform for our public/private partnership. For more information on the 405(d) Program please email us at CISA405d@hhs.gov !

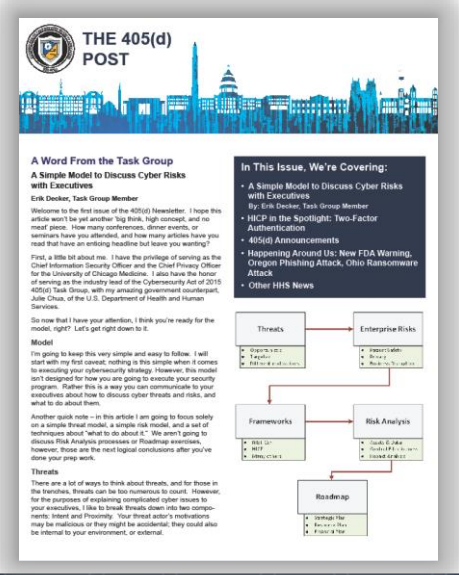


405(d) Resources

405(d) Awareness Materials

The 405(d) Program periodically creates awareness materials that can be utilized in any size organization! These 5 threat posters were created in support of Cybersecurity Awareness Month in October 2019 to be used in hospitals, doctors office's and even in email threads!





405(d) Outreach

The 405(d) Program produces Bi-monthly Newsletters and Spotlight Webinars to increase cybersecurity awareness and present on new and emerging cybersecurity news and topics, as well highlighting the HICP Publication!

405(d) Social Media

The 405(d) Program is now live on Twitter, Instagram, and Facebook at @ask405d. Follow us to receive up to date 405(d) News and cybersecurity tips and practices!

Healthcare delivery organizations common cybersecurity threats

COVID-19 era

Common cybersecurity threats to health care organizations

Cybercriminal and advanced persistent threat (APT) groups

Health Industry Cybersecurity Practices (HICP) - December 2018

The **5 current threats** identified in healthcare:

1. Email Phishing Attacks
2. Ransomware Attacks
3. Loss or Theft of Equipment or Data
4. Internal, Accidental or Intentional Data Loss
5. Attacks Against Connected Medical Devices That May Affect Patient Safety

June 2020

1. **Phishing lure**
2. **Ransomware**
3. **Data Theft – remote malicious code deployment**
4. **Exploitation of remote access and teleworking infrastructure**
5. **Attacks against unmanaged devices (medical devices, IoT, cloud instances, etc.)**

Common cybersecurity threats to health care organizations

COVID19 era

Phishing lure

- Dramatic increase of spam and scams
- +260% Increase in malicious URL hits
- Gmail: >18 million daily phishing emails related to COVID-19

Malicious code deployment

- >1K COVID-19 confirmed marlware variants
- Hackers seek to steal coronavirus research
- Hospitals, laboratories, healthcare providers and pharmaceutical companies all been hit

Ransomware

- 33% increase in average ransom payments issued
- Spike in “Double Extortion” ransomware attacks
- Targeting personal (i.e. mobile phone) and organizational devices

Remote & teleworking infrastructure

- VPN One-Day vuln exploitation (Citrix, Pulse Secure)
- Cloud collaboration services (i.e. Office365)
- Password spraying (i.e. RDP)

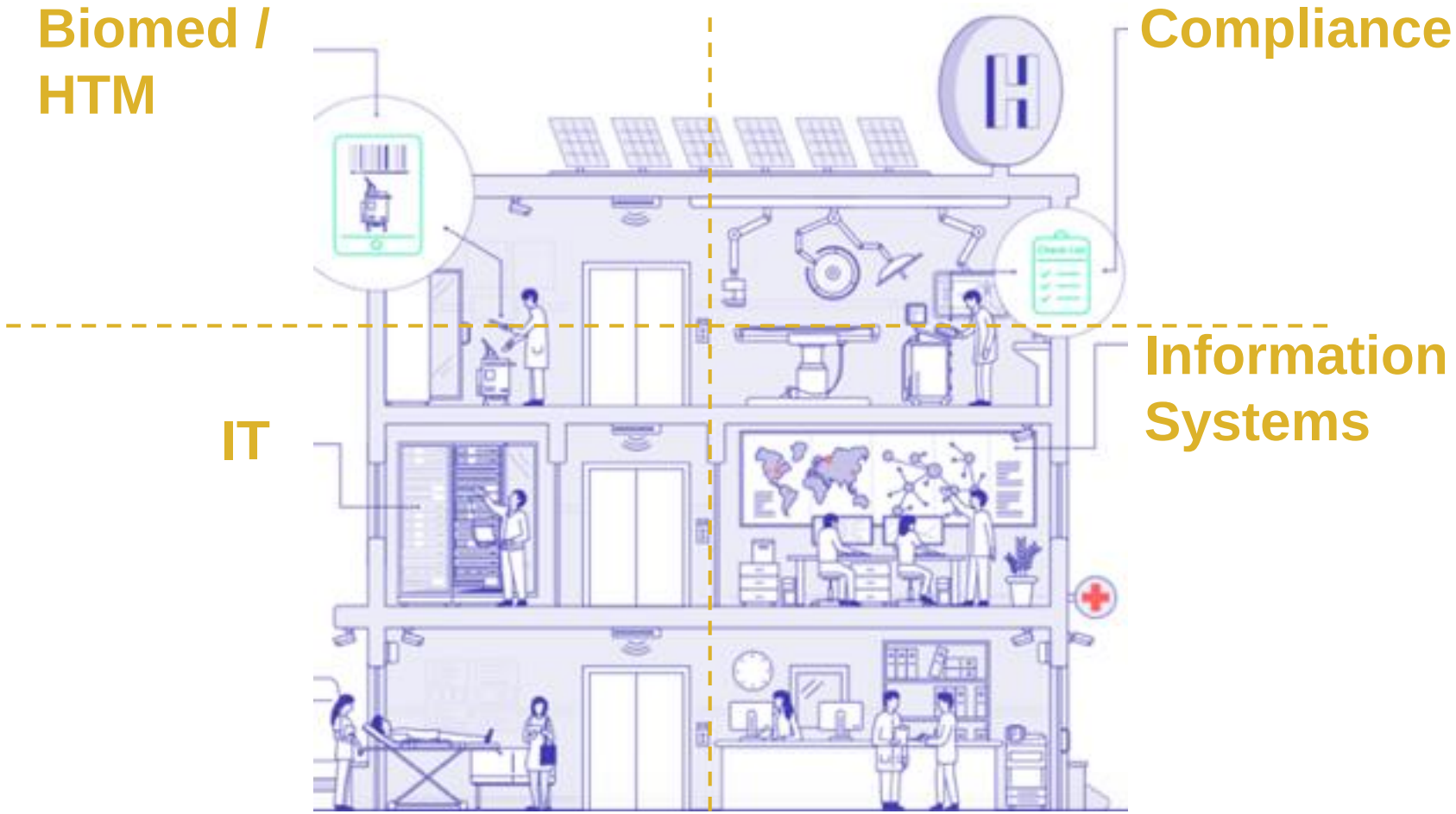
Unmanaged device attacks

- Medical devices, IoT & OT (default credentials, unpatched and legacy software)
- Often rapidly deployed

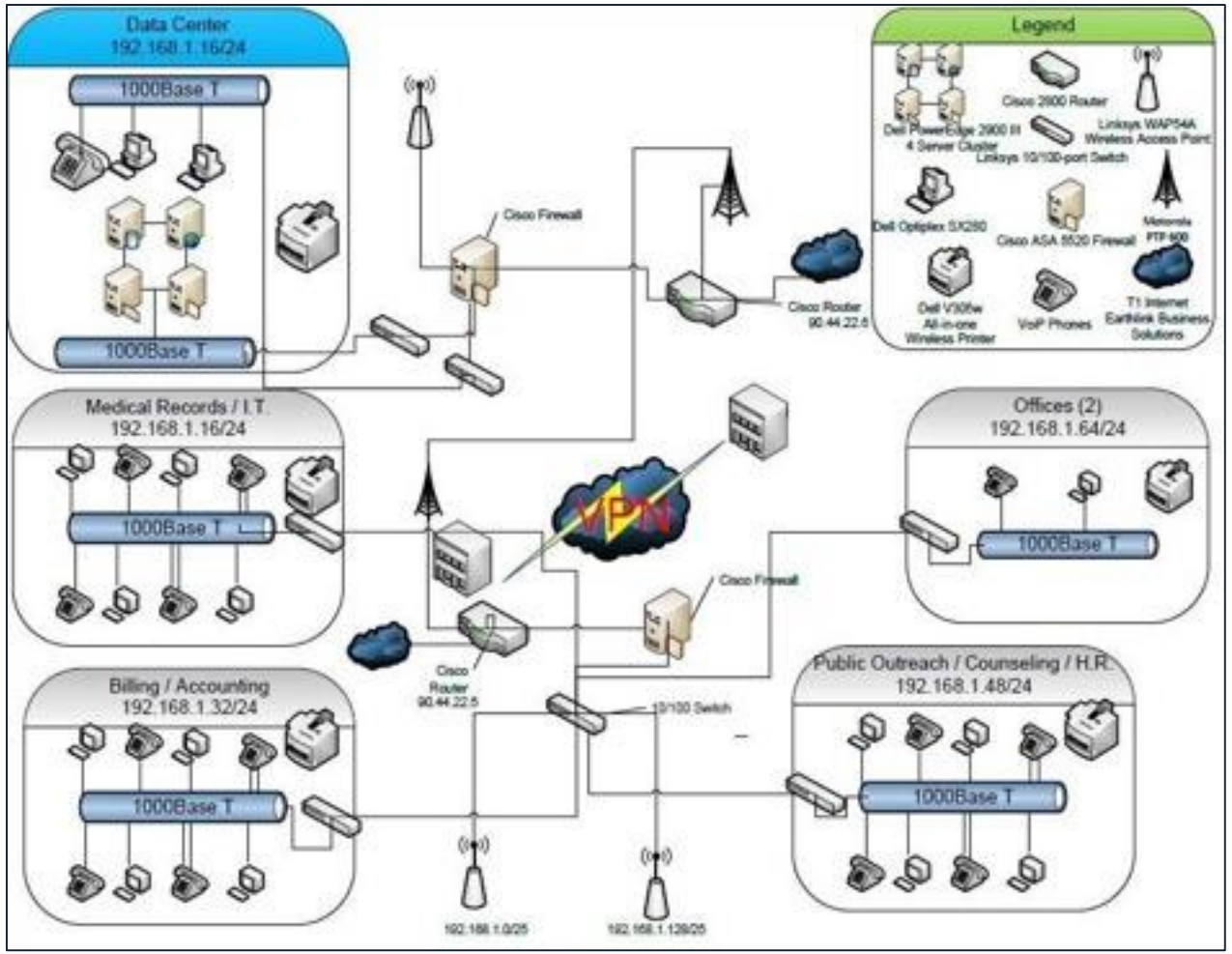
United States

Top location for spam, malware detections, and users accessing malicious URL’s

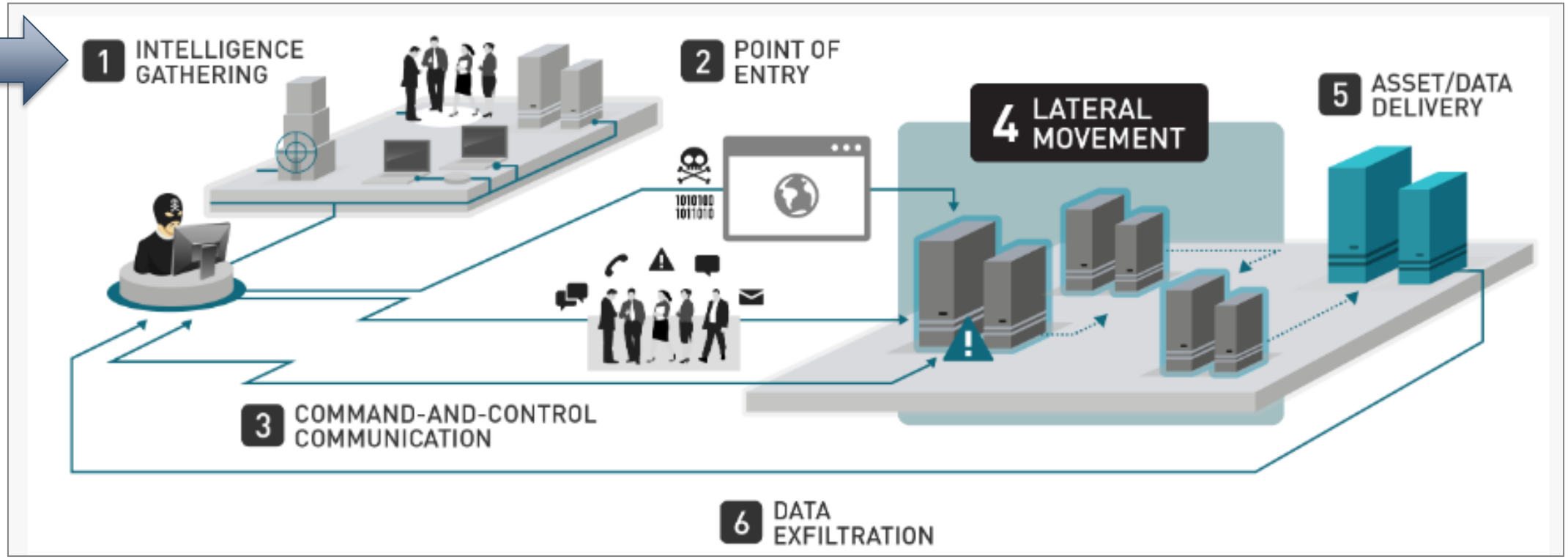
How internal healthcare teams see a hospital



How a hacker sees a hospital

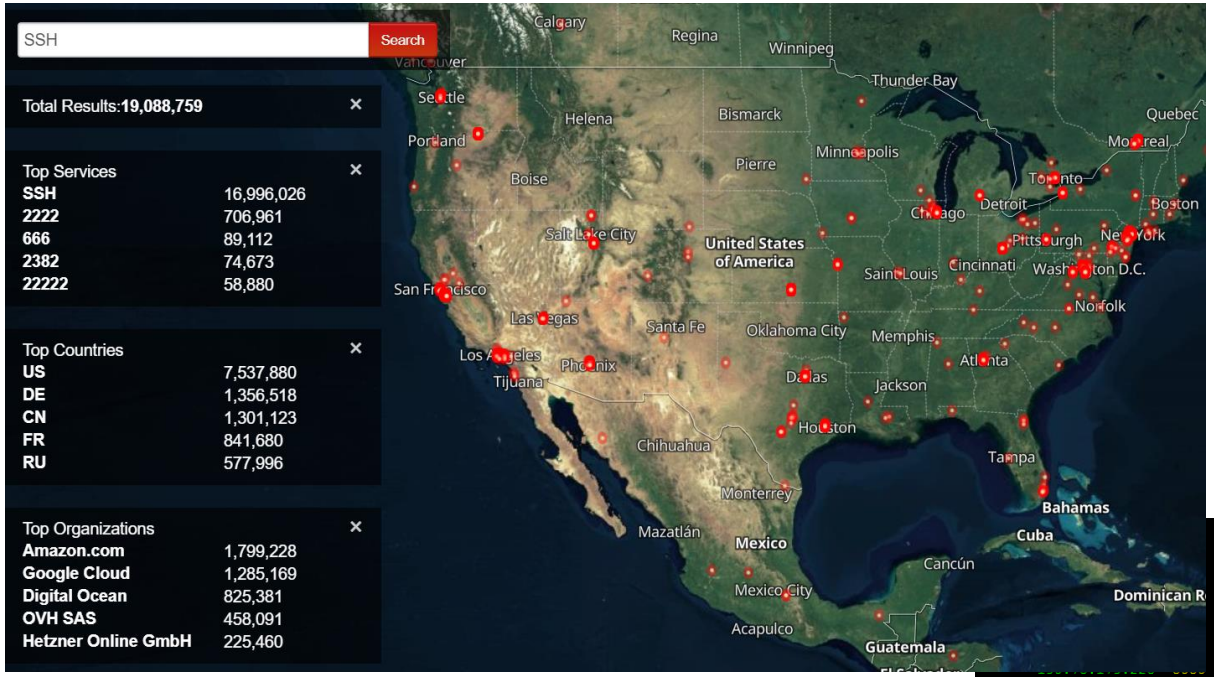


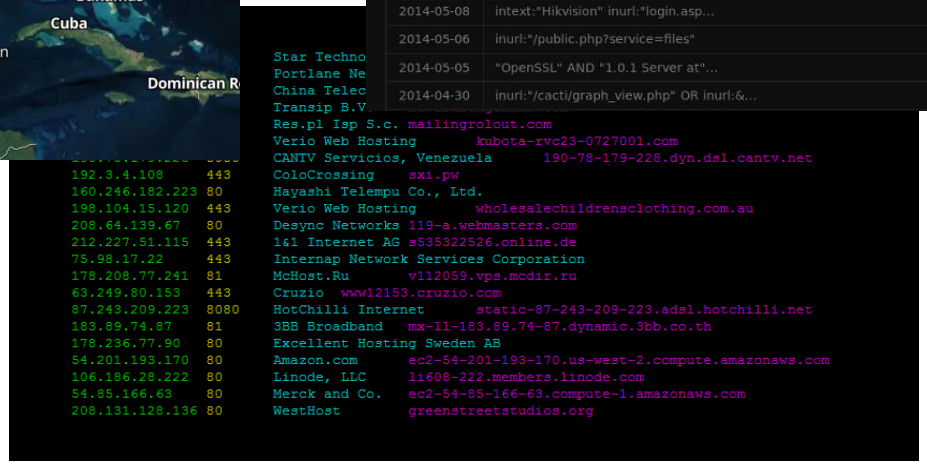
Cyber attack phases



Intelligence gathering / Reconnaissance

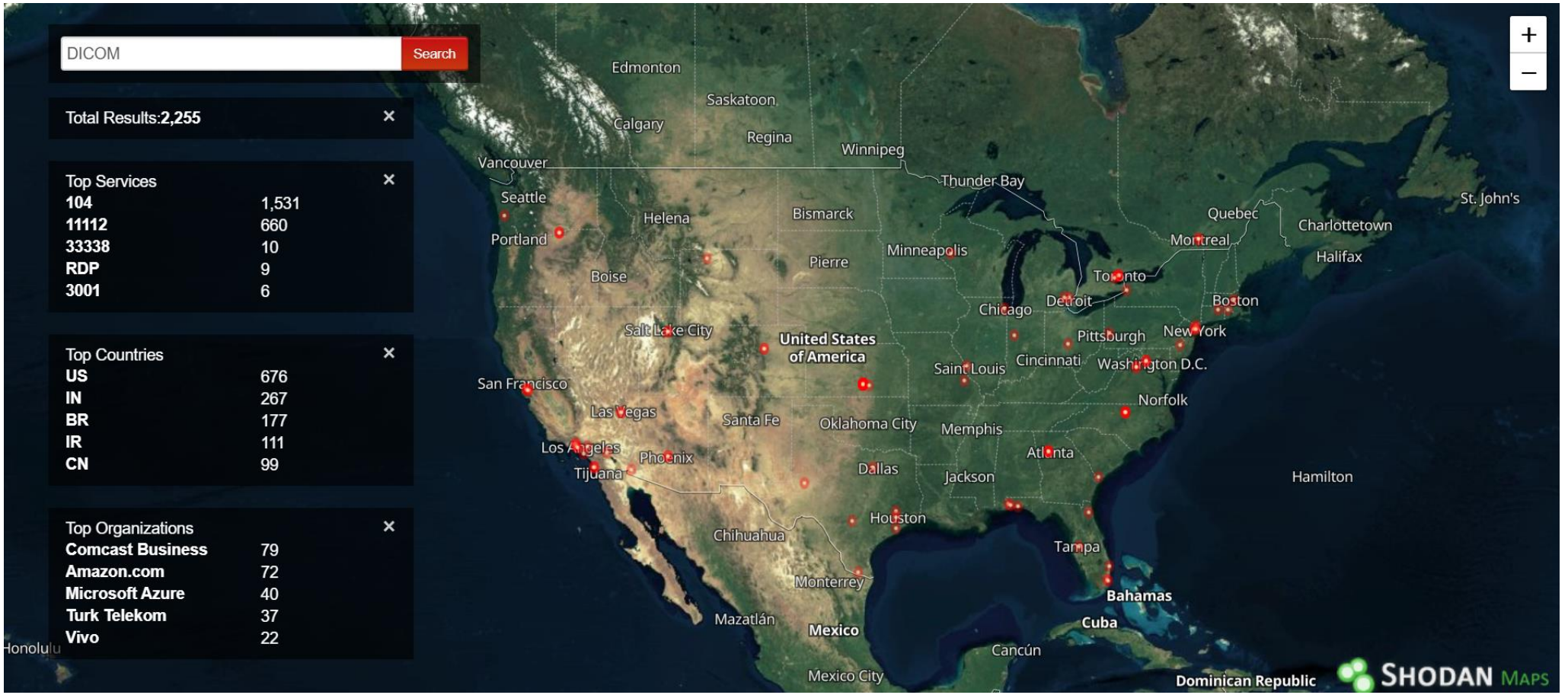
Many tools accessible with a simple Google search



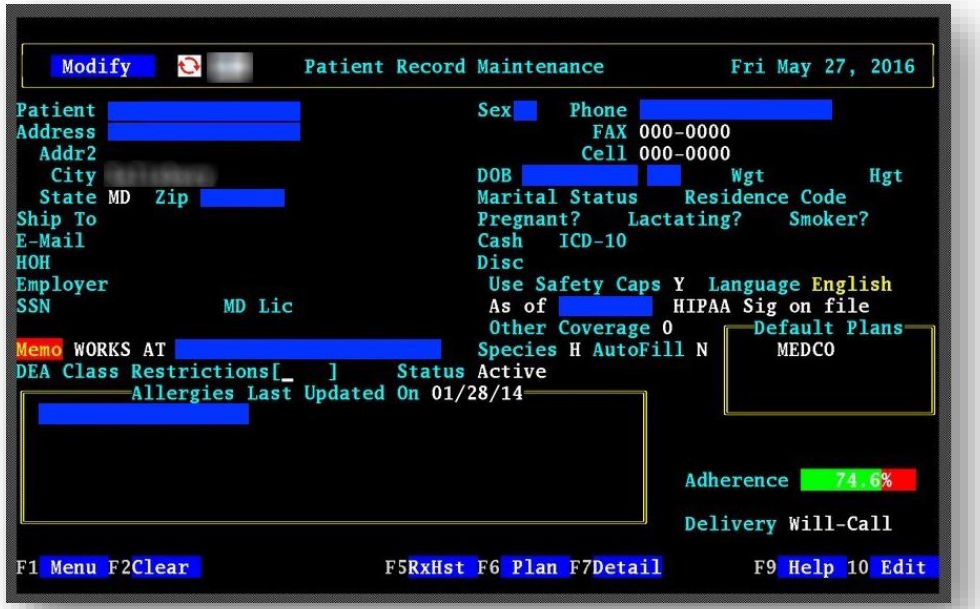


Internet exposed medical systems

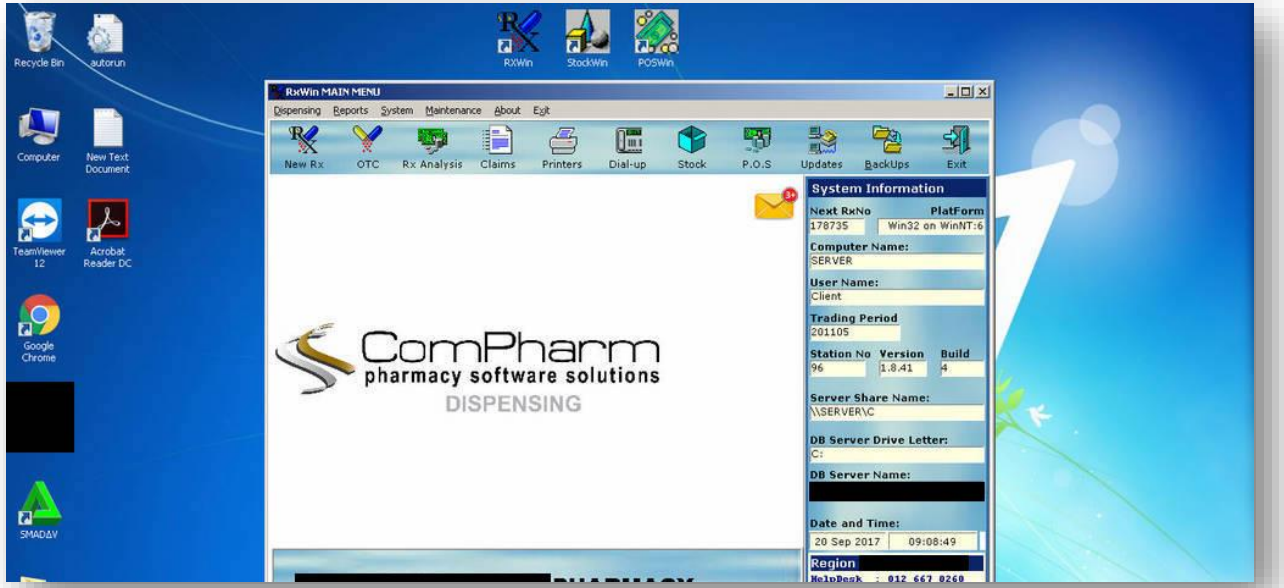
DICOM Servers



Internet exposed medical systems

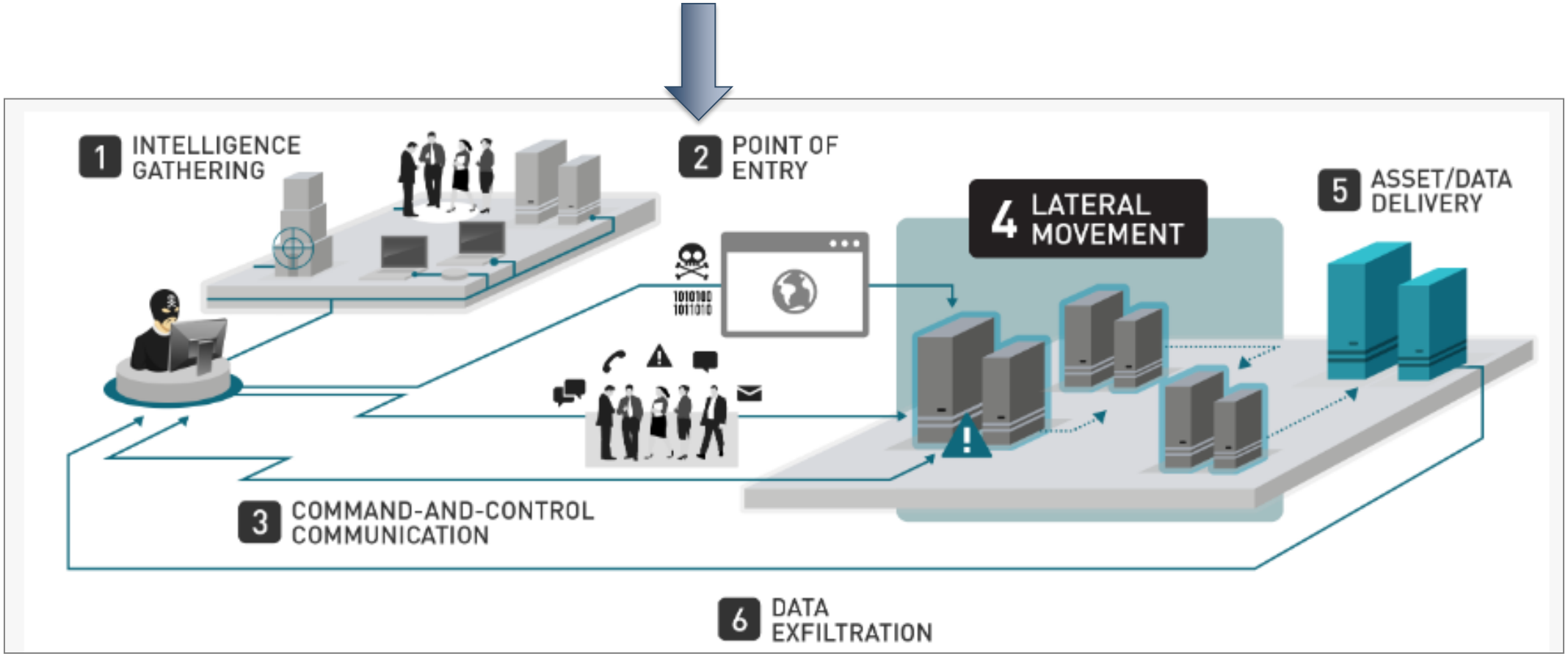


Exposed user interface for patient record maintenance containing ePHI



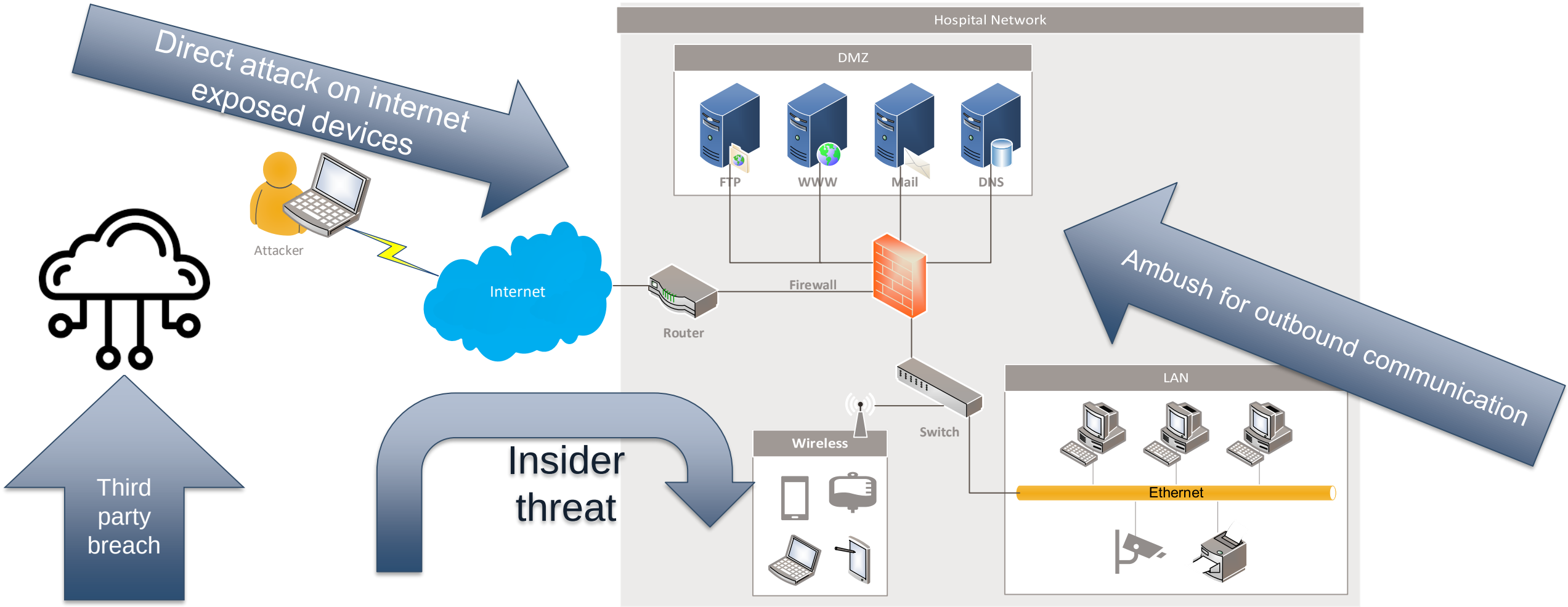
Exposed pharmacy management software GUI

Attack phases



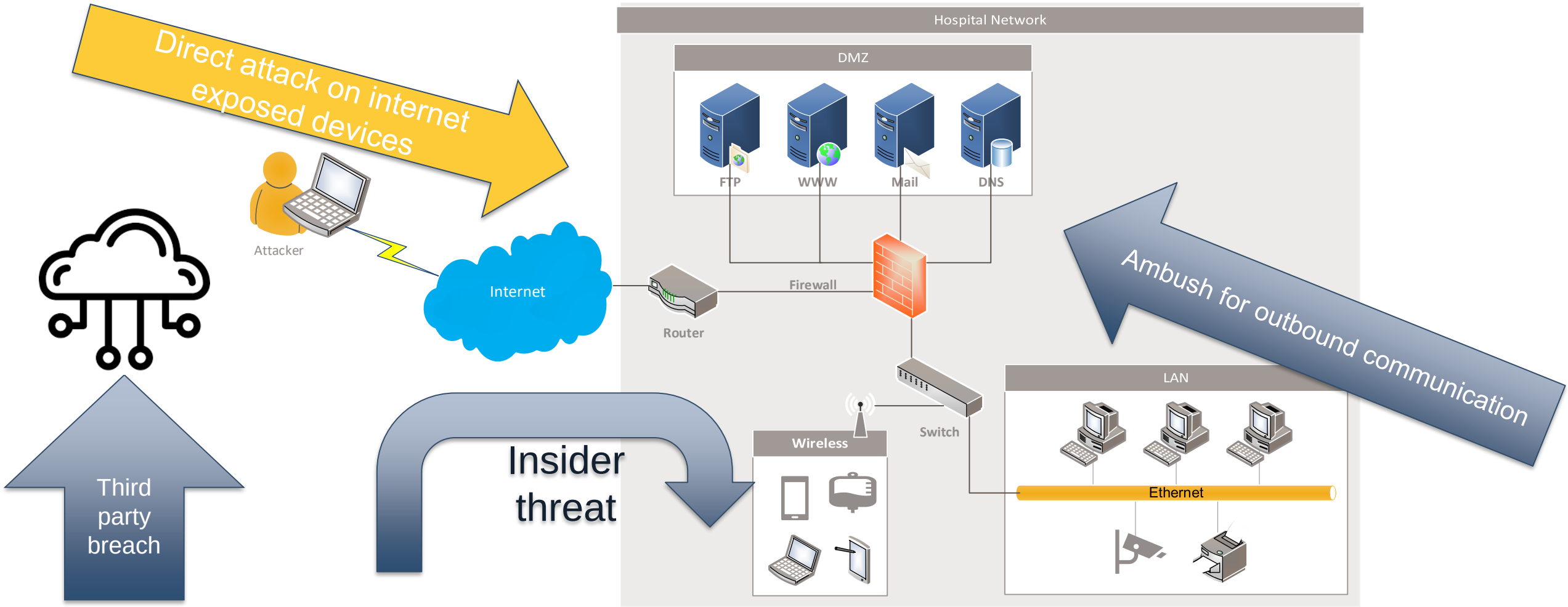
Points of entry

How the attacker can infiltrate your organization



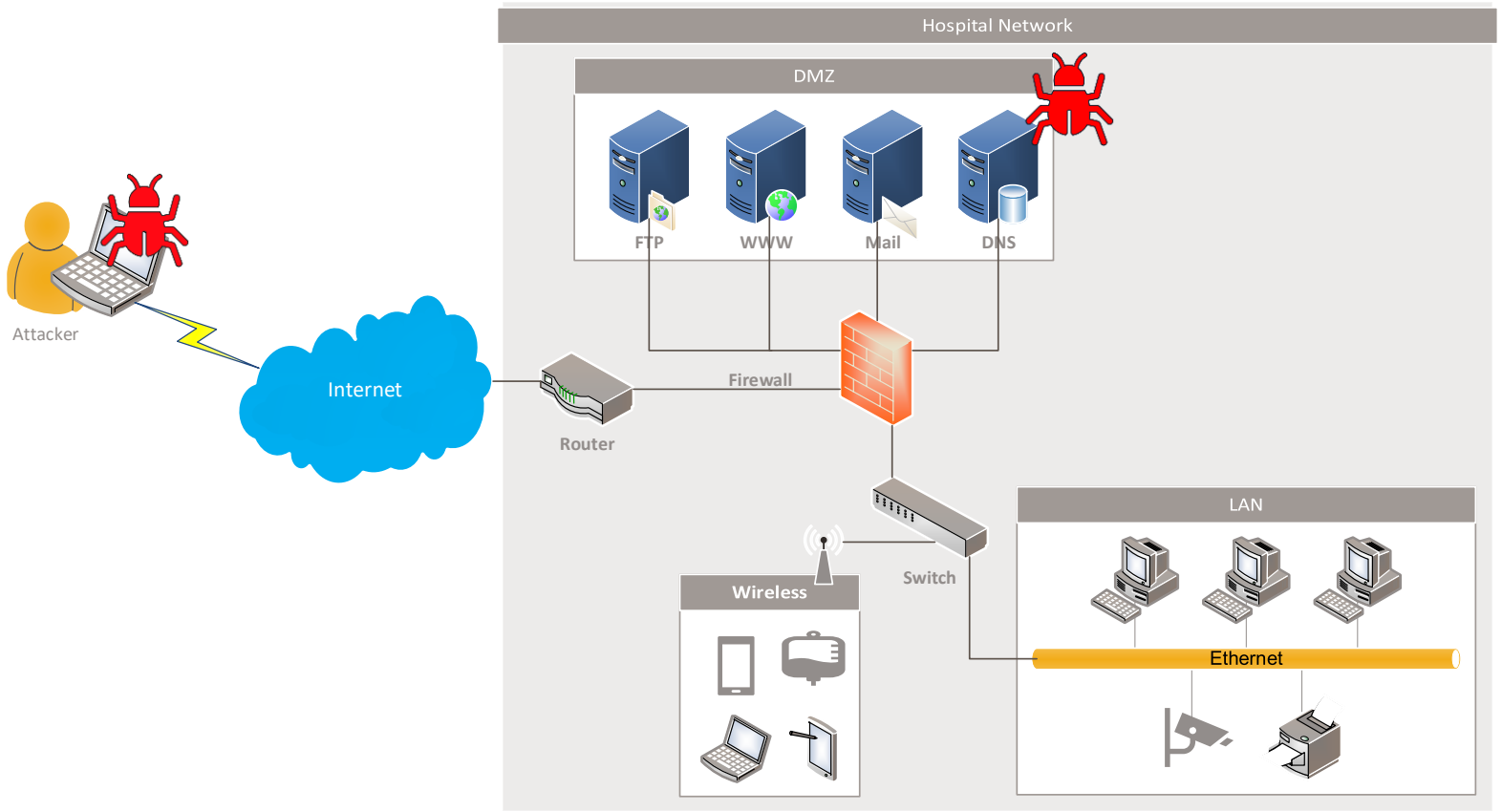
Points of entry

How the attacker can infiltrate your organization



Point of entry

Direct attack on internet exposed devices



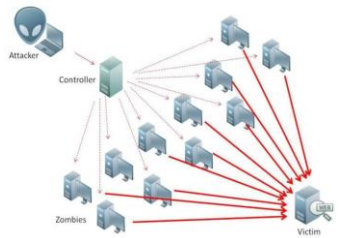
Direct attack on internet exposed devices

Healthcare breaches - common use cases

Google Hacking

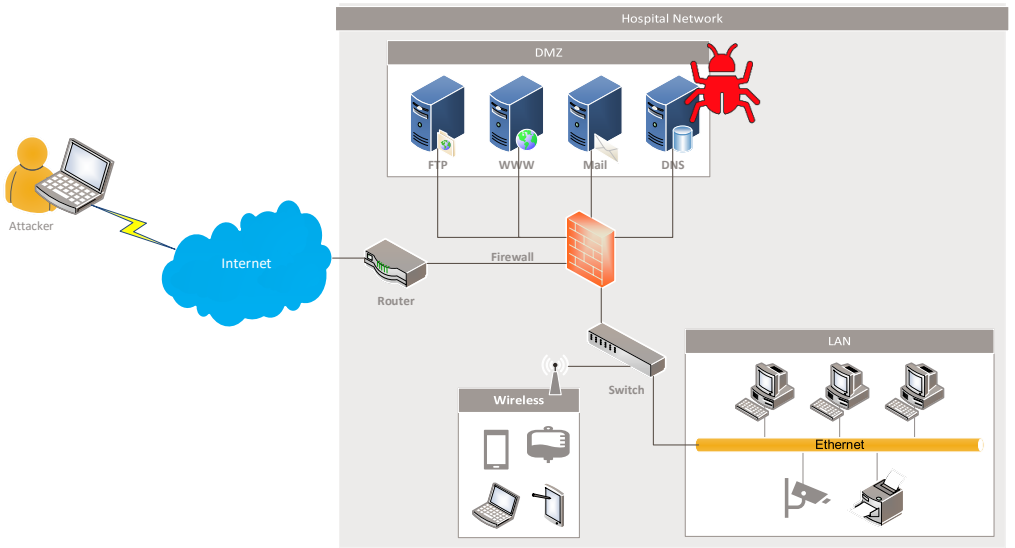
Web Application Hacking

Vulnerabilities Exploitation



Denial of Service

Password Attack



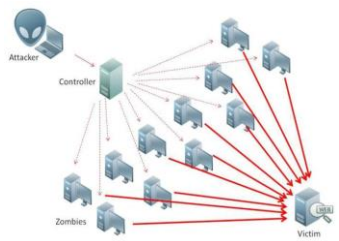
Direct attack on internet exposed devices

Healthcare breaches - common use cases

Google Hacking

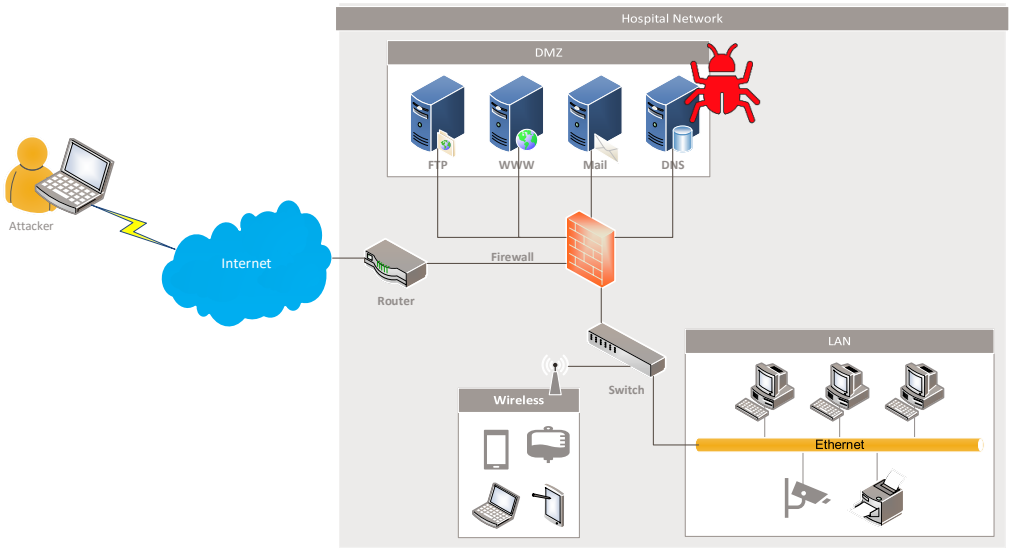
Web Application Hacking

Vulnerabilities Exploitation



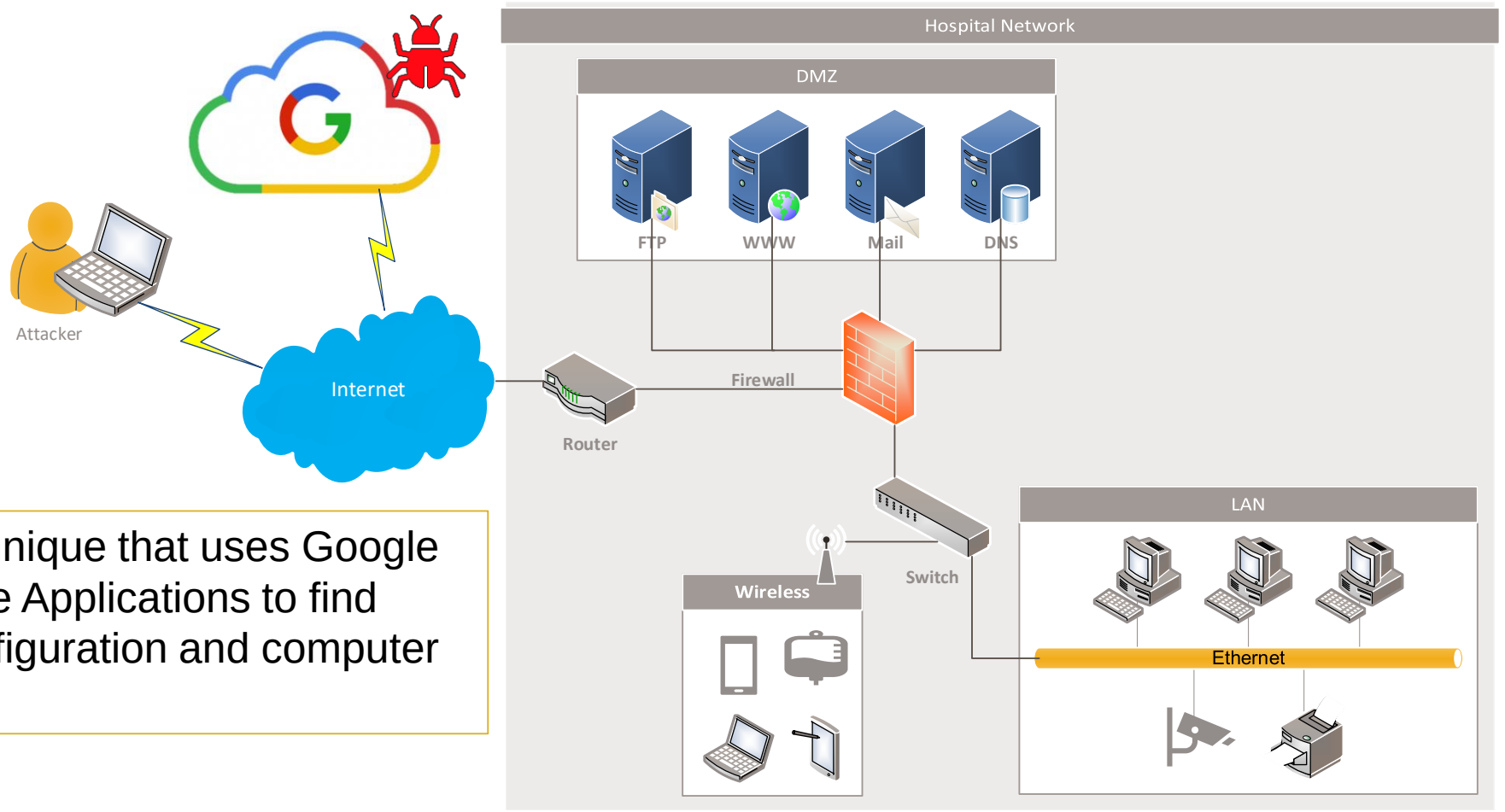
Denial of Service

Password Attack



Direct attack on internet exposed devices

Google hacking

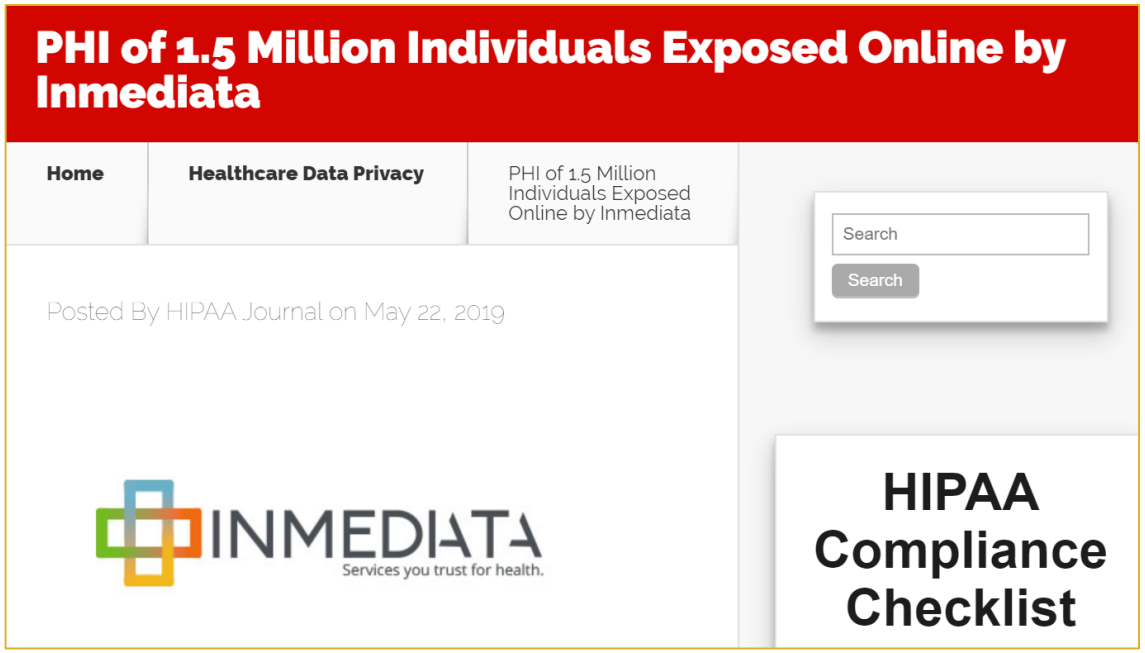


A computer hacking technique that uses Google Search and other Google Applications to find security holes in the configuration and computer code that websites use

Direct attack on internet exposed devices

Google hacking

- A **misconfigured database** led to a personal health data breach of 1.57 million Inmediata Health Group patients
- The misconfiguration allowed search engines to **index internal Inmediata webpages used for business operations**



Direct attack on internet exposed devices

Google hacking

- A **misconfigured database** belonging to NJ-based Home Health Radiology, contained sensitive data of about 37,000 patients exposed to the internet
- Stored on an **Elastic database that was not password-protected and could be accessed over the internet**

- University of Washington Medicine **974,000 patient data was exposed online due to a misconfigured server**
- The breach was discovered in December 2018 when **a patient conducted a search of their own name and found a file containing their personal information**

Direct attack on internet exposed devices

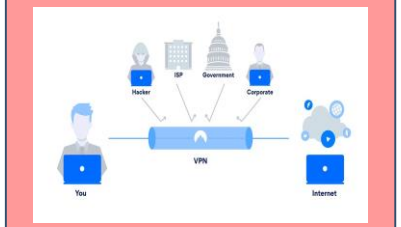
Healthcare breaches - common use cases

Google HACKING

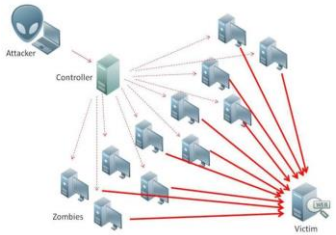
Google Hacking

Web Application Hacking

Vulnerabilities Exploitation

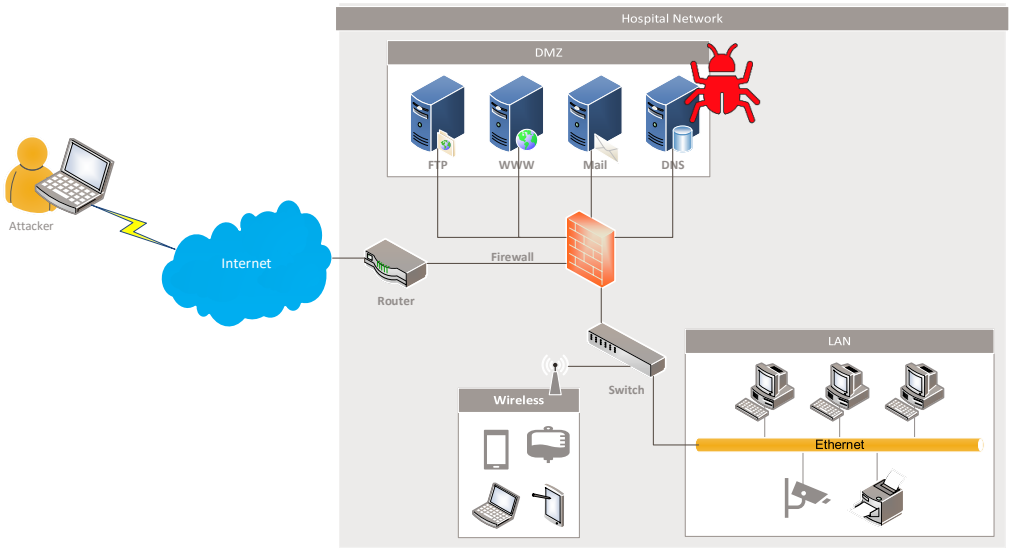


Remote & teleworking infrastructure



Denial of Service

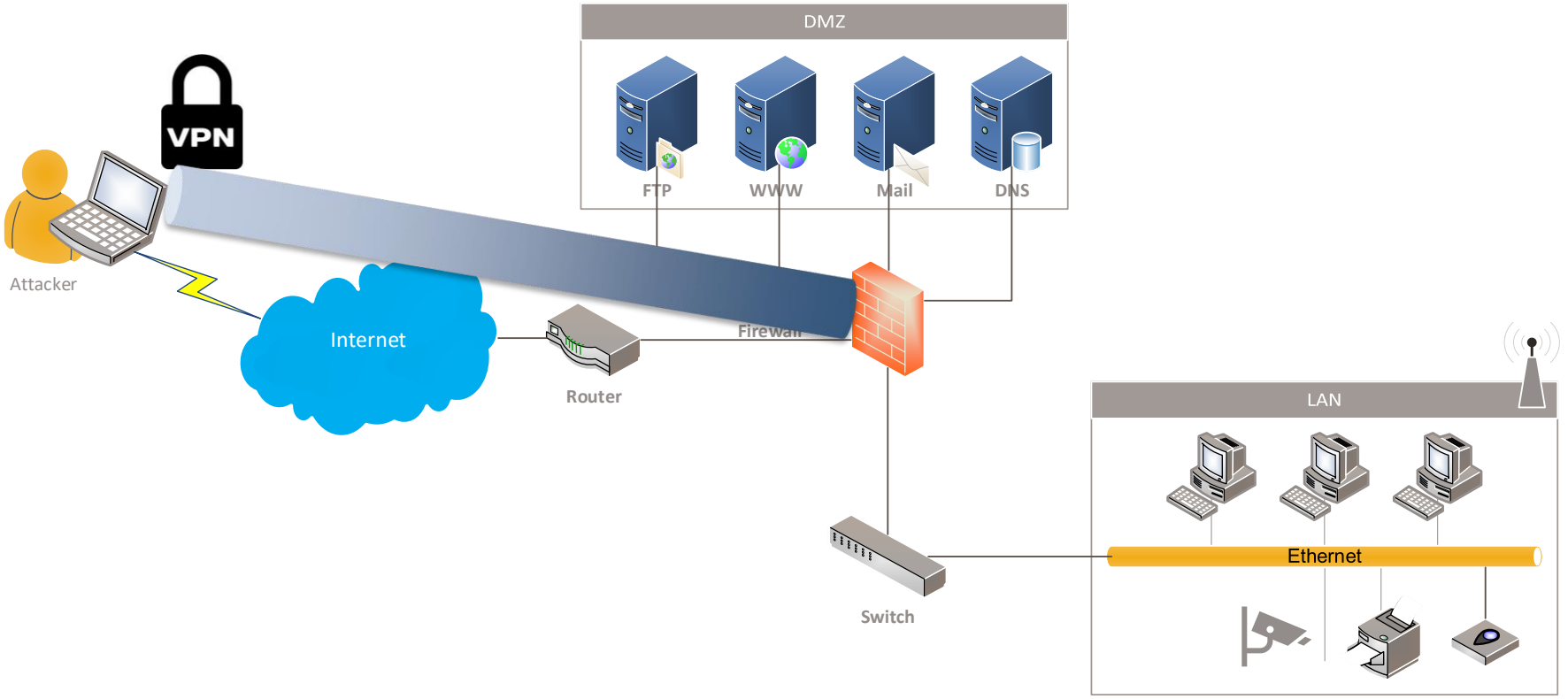
Password Attack



Direct attack on internet exposed devices

Remote & teleworking infrastructure -> vulnerability exploitation -> hacking into VPN Connections

VPNs work by creating a **secure virtual tunnel through the Internet to another network or device**



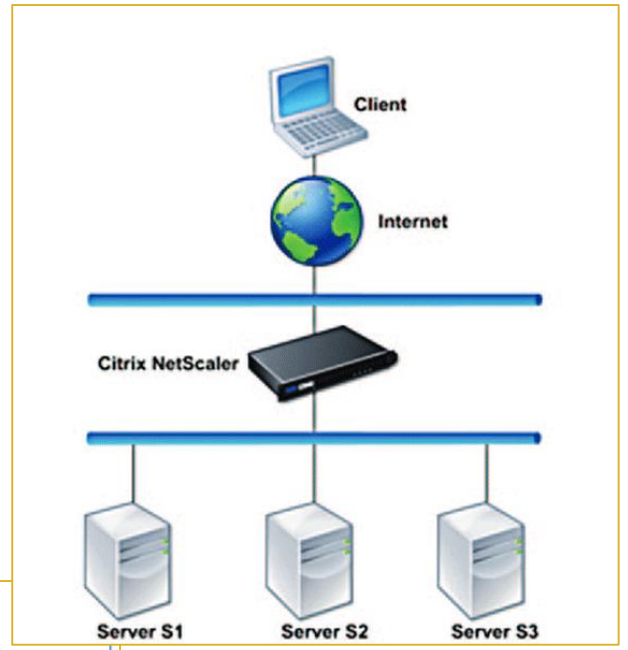
Direct attack on internet exposed devices

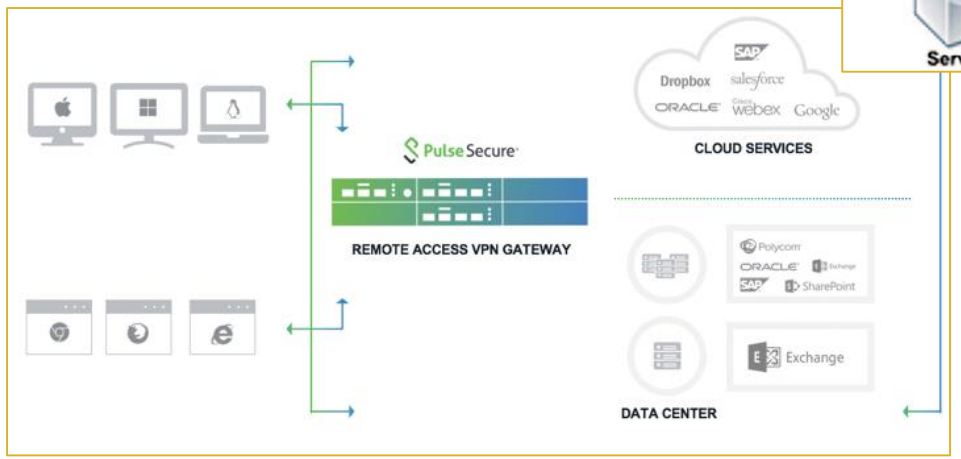
Hacking into VPN Connections

US-CERT Alert (AA20-126A) - May 05, 2020

APT actors scanning the external domains of targeted companies and looking for vulnerabilities.

Actors are known to take advantage of Citrix vulnerability (CVE-2019-19781) and Pulse Secure VPN servers vulnerabilities.

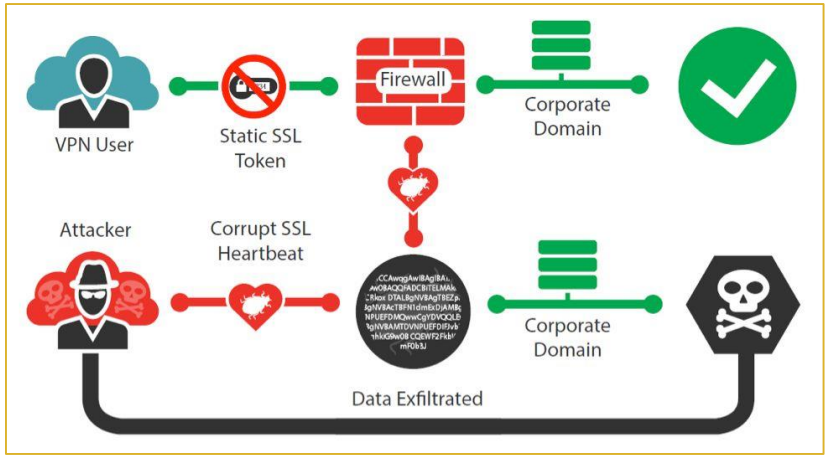




Direct attack on internet exposed devices

Point of Entry->vulnerability exploitation->lateral movement->data exfiltration

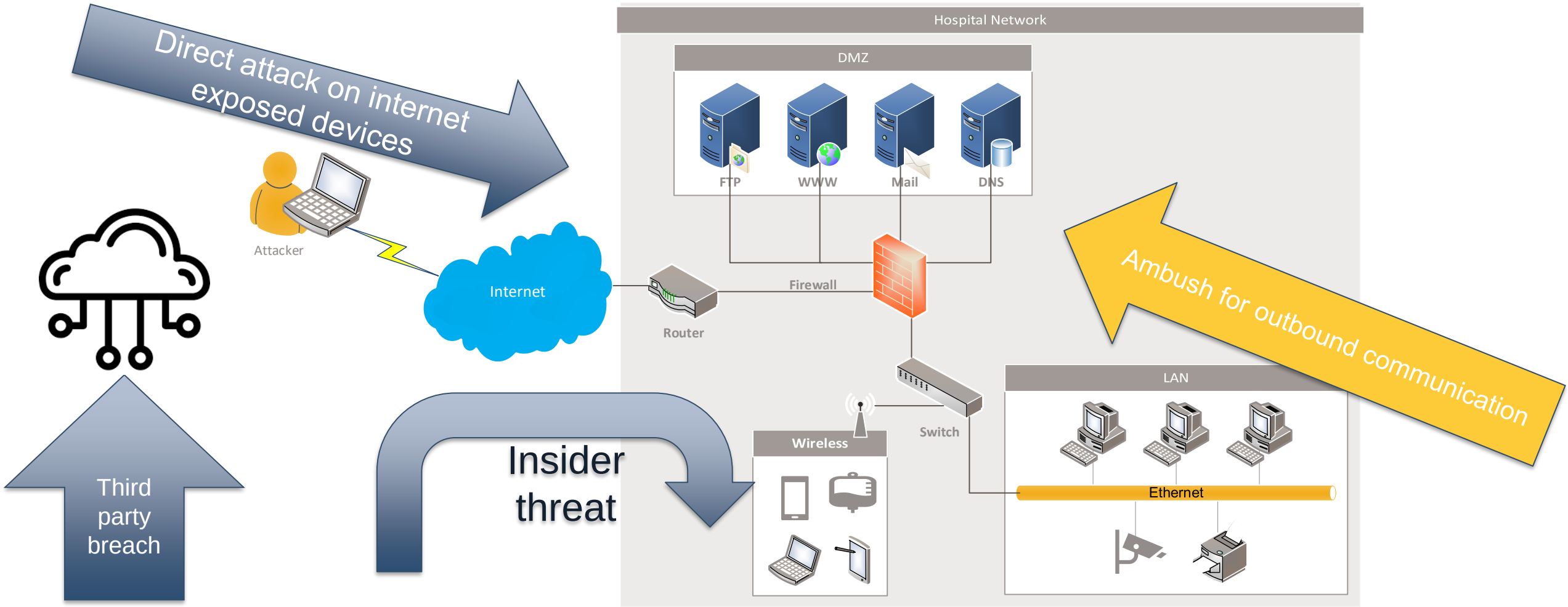
- Attackers leveraged **Heartbleed vulnerability (CVE-2014-0160)** and **gain user credentials** from a Juniper device on the Community Health Systems network
  - The **credentials were used to login to the company's VPN**
- Once connected to the VPN, the attacker moved laterally and escalate their privileges within the organization
  - They hacked their way into a database and **stole millions of ePHI records**
- The attack seems to be the work of an advanced persistent threat (APT) group



Heartbleed Vulnerability

Points of entry

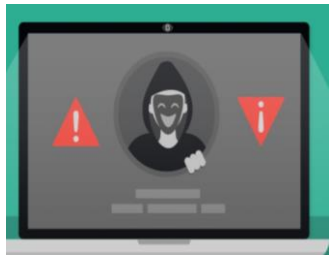
How the attacker can infiltrate your organization



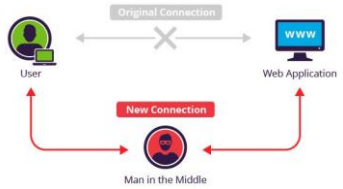
Ambush for outbound communication

Healthcare attacks common use cases

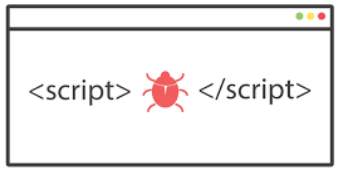
Phishing



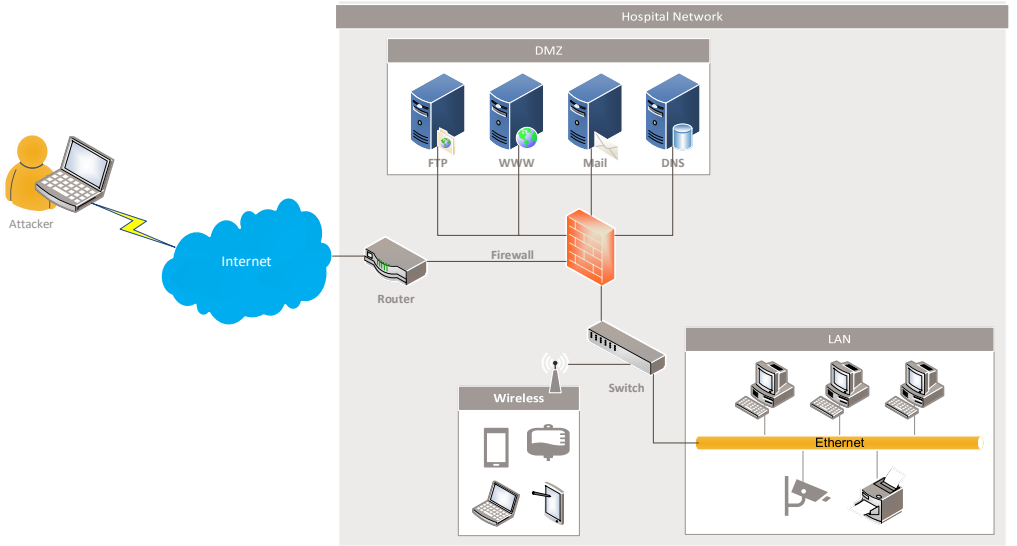
Watering Hole



Man In the Middle



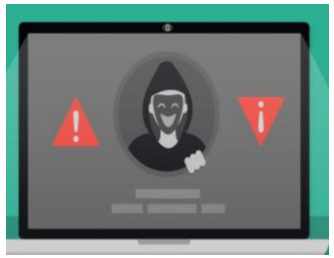
Cross-site scripting (XSS)



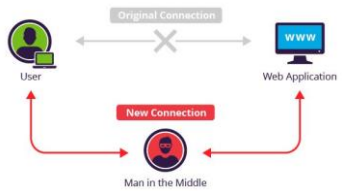
Ambush for outbound communication

Healthcare attacks common use cases

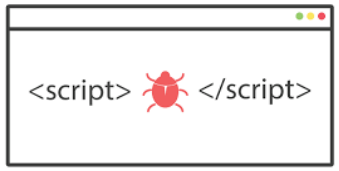
Phishing



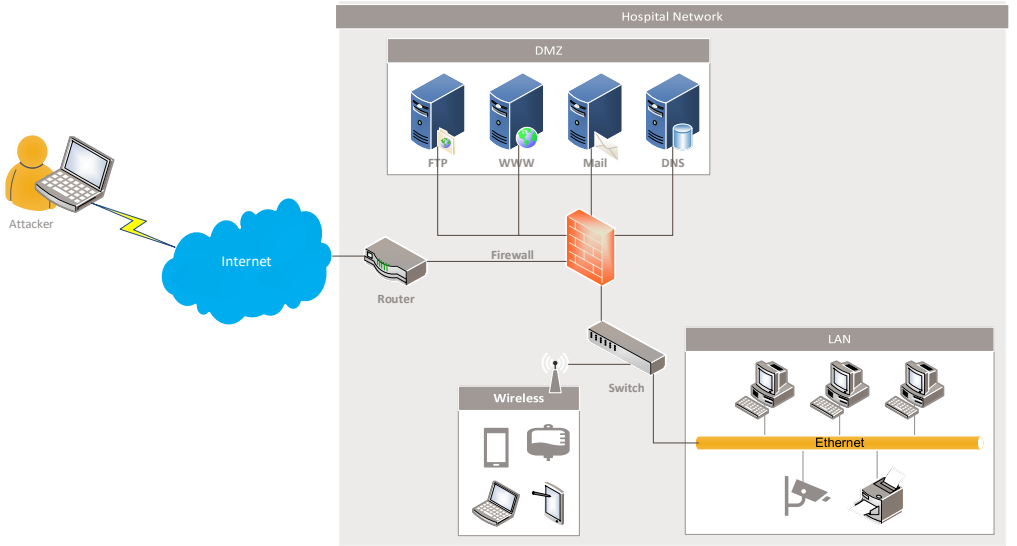
Watering Hole



Man In the Middle

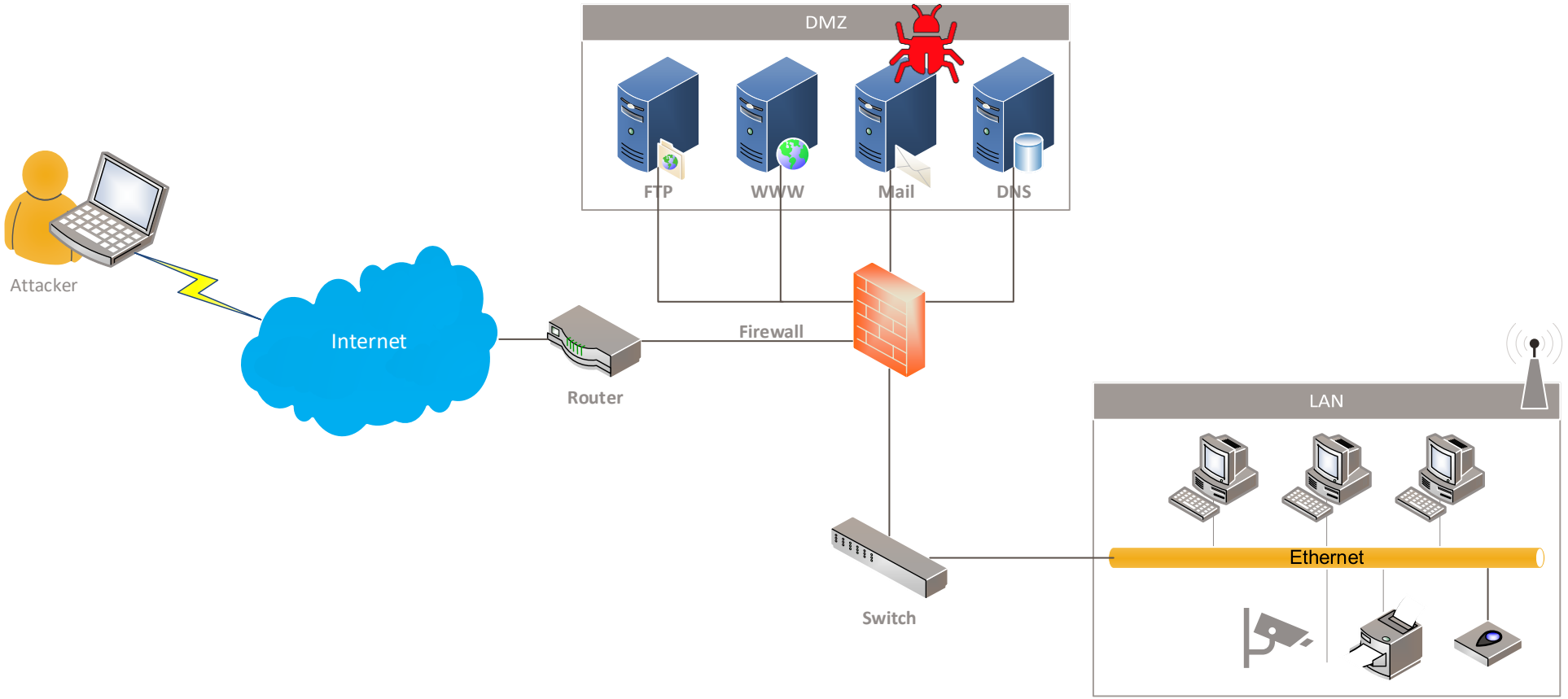


Cross-site scripting (XSS)



Ambush for outbound communication

Phishing attack



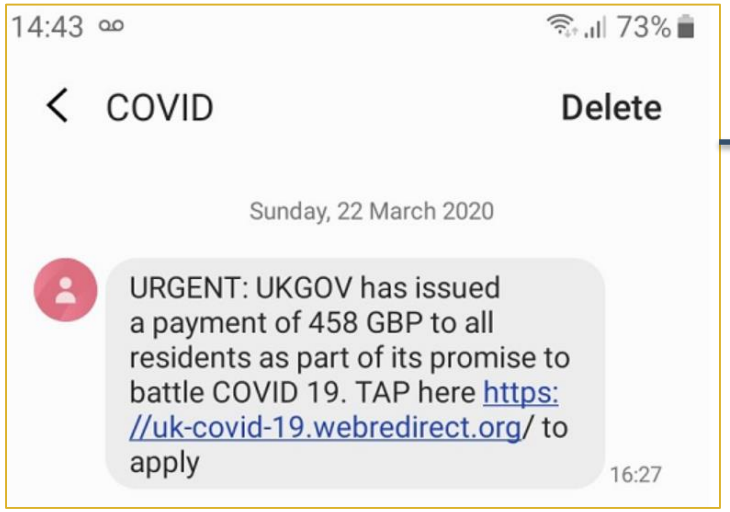
Ambush for outbound communication

Phishing attack lure

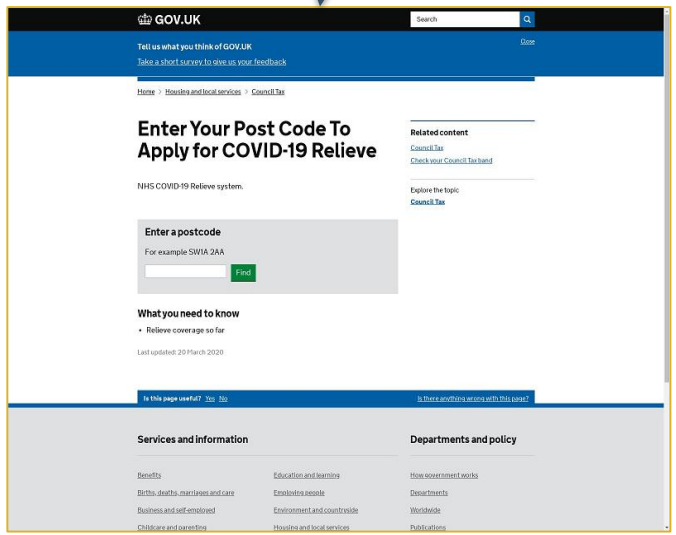
Phishing is a cybercrime in which targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data and/or clicking on a malicious link or attachment

Ambush for outbound communication

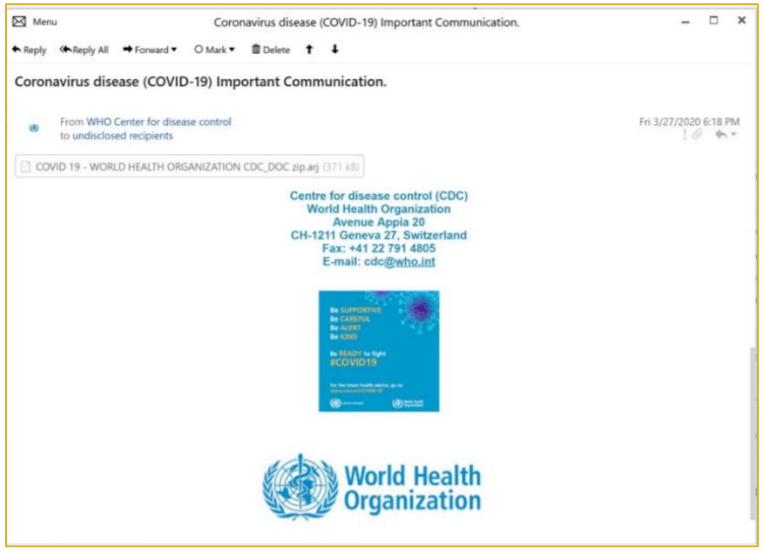
Phishing attack lure – Covid19 era



UK government SMS phishing-themed



UK government-themed phishing page

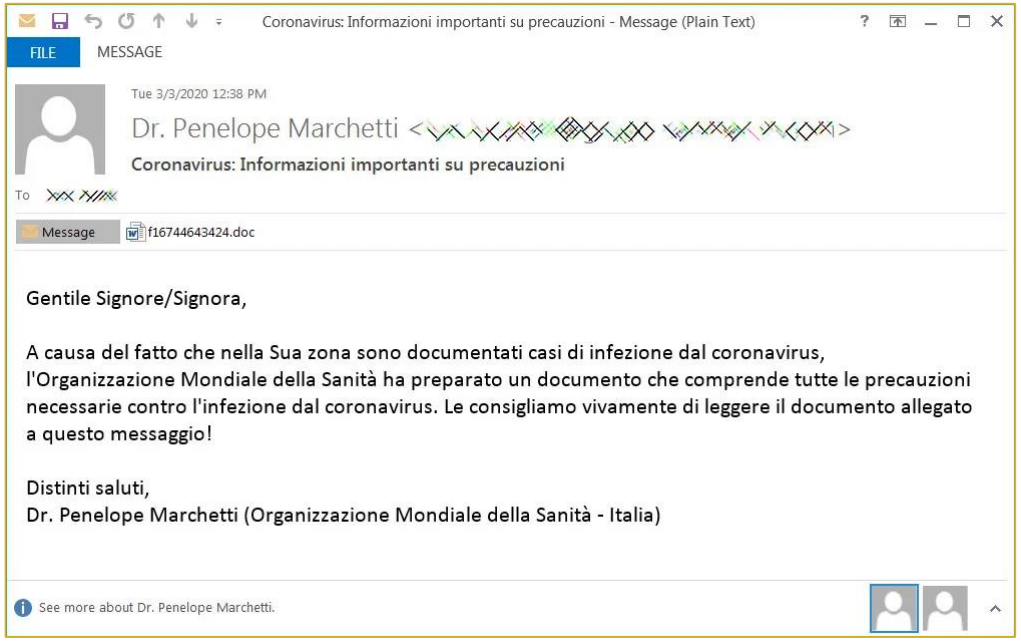


Coronavirus-themed spear phishing email that uses the WHO trademark

Ambush for outbound communication

Spear phishing coronavirus-themed

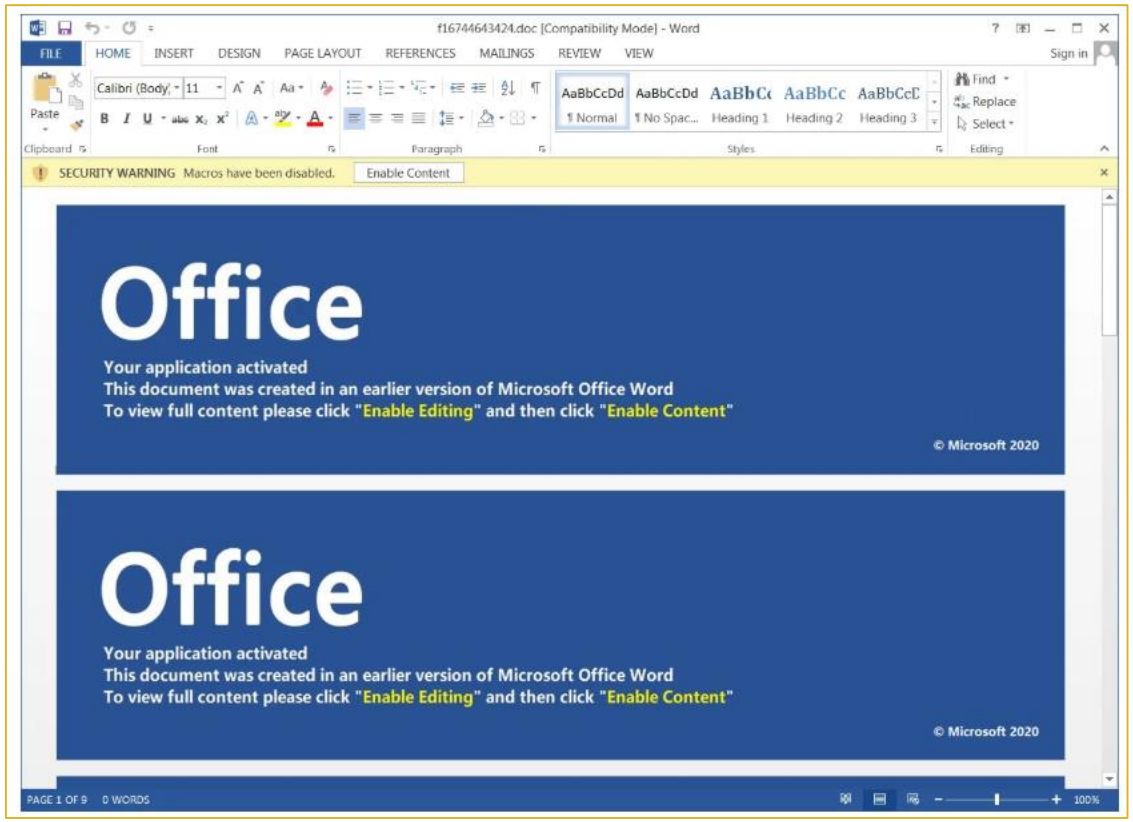
- Email **claims to provide** information about precautions people in Italy should take to **protect themselves from the Coronavirus**



Ambush for outbound communication

Spear phishing coronavirus-themed

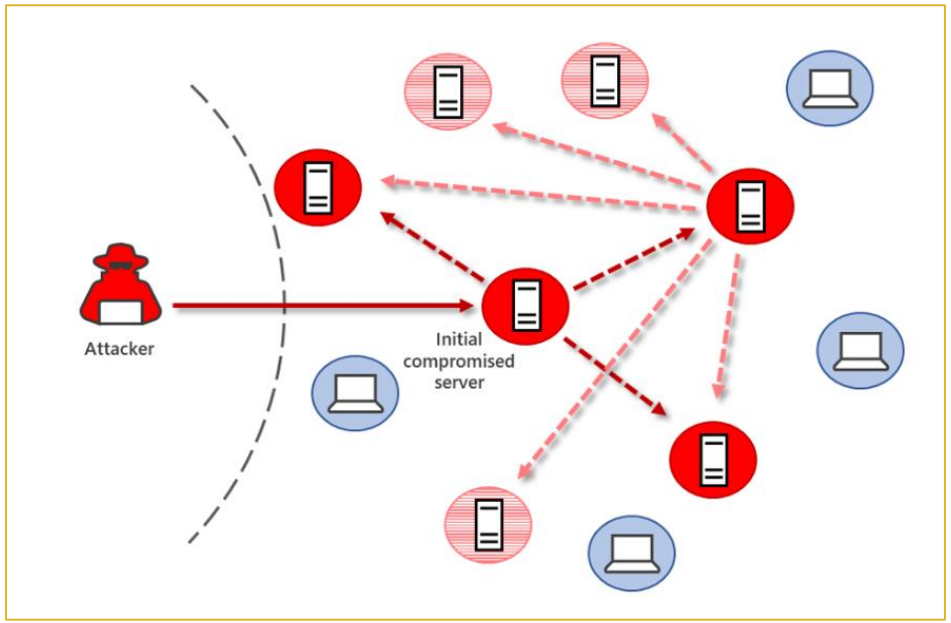
- Email **claims to provide** information about precautions people in Italy should take to **protect themselves from the Coronavirus**
- **Attached is a malicious Word document**
- Once someone open the content in Word and clicks on “Enable Content”, **malicious** macros are executed that **install Trickbot malware**



Ambush for outbound communication

Spear phishing coronavirus-themed

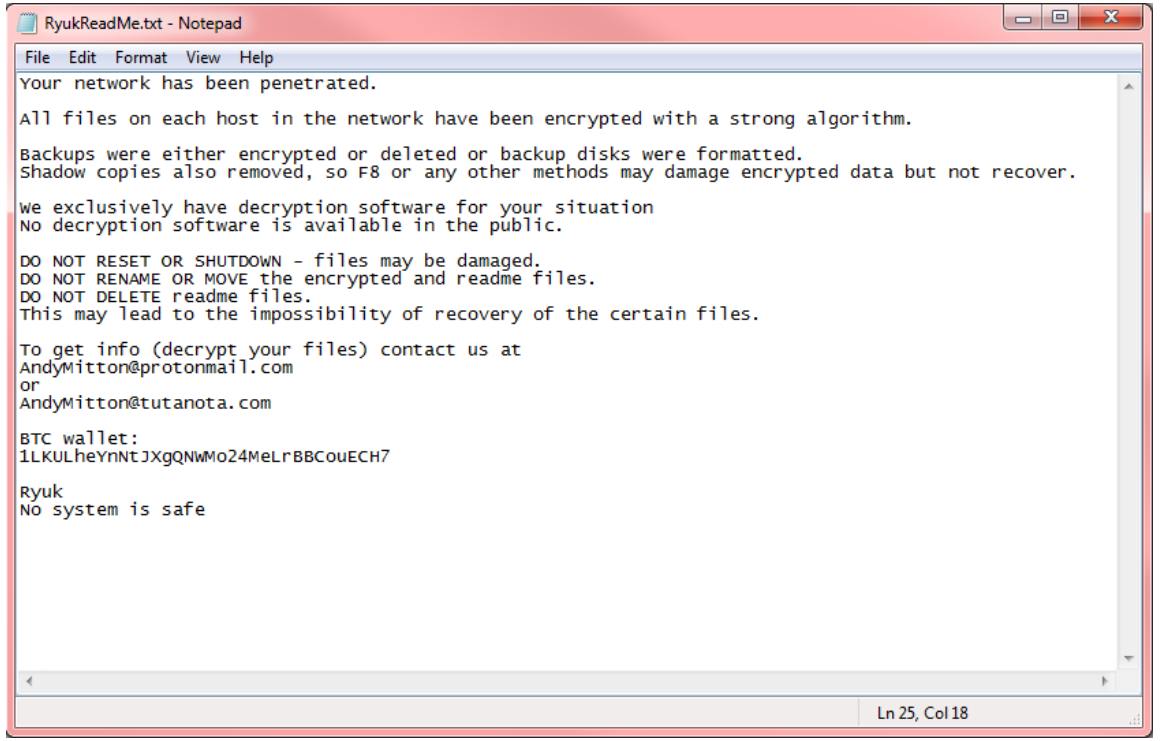
- Email **claims to provide** information about precautions people in Italy should take to **protect themselves from the Coronavirus**
- **Attached is a malicious Word document**
- Once someone open the content in Word and clicks on “Enable Content”, **malicious** macros are executed that **install Trickbot malware**
- The Malware **harvests information from a compromised endpoint** and then attempts to **spread laterally** throughout the network



Ambush for outbound communication

Spear phishing coronavirus-themed

- Email **claims to provide** information about precautions people in Italy should take to **protect themselves from the Coronavirus**
- **Attached is a malicious Word document**
- Once someone open the content in Word and clicks on “Enable Content”, **malicious** macros are executed that **install Trickbot malware**
- The Malware **harvests information from a compromised endpoint** and then attempts to **spread laterally** throughout the network
- After reconnaissance of the network, gaining admin credentials and stealing data, the hackers will deploy the Ryuk **Ransomware and encrypt the files of all the compromised endpoints on the network**



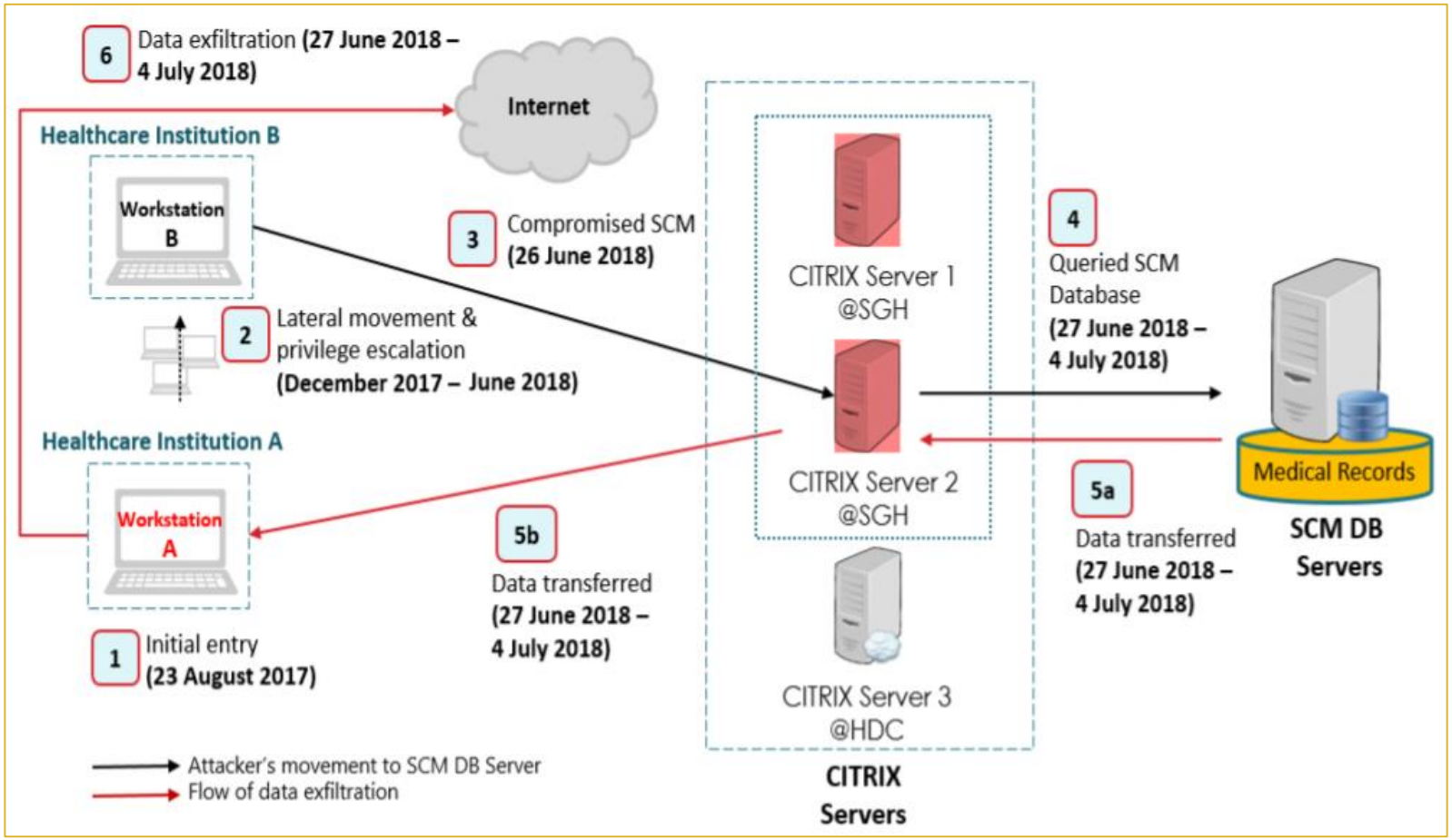
Singapore’s breach

Phishing->vulnerability exploitation->lateral movement->data exfiltration

- The crown jewels of the SingHealth network are the **patient electronic medical records**
- After the **initial reconnaissance** of the hackers, the operatives sent **booby-trapped emails** to Singhealth employees
- The trap consisted in a **malicious attachment capable of exploiting a known Outlook vulnerability**
- When opened, the attachment launched a malicious code on the victims’ systems
- The rest of the attack consisted **of using legitimate accounts to query databases and scour resources**, like one on their own systems, until they found what they were looking for

Singapore's breach

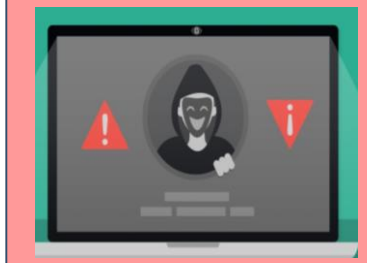
Phishing->vulnerability exploitation->lateral movement->data exfiltration



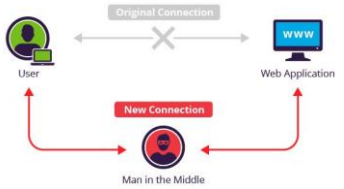
Ambush for outbound communication

Healthcare attacks common use cases

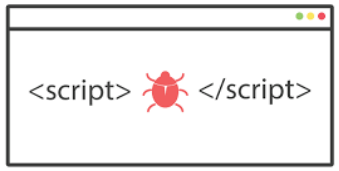
Phishing



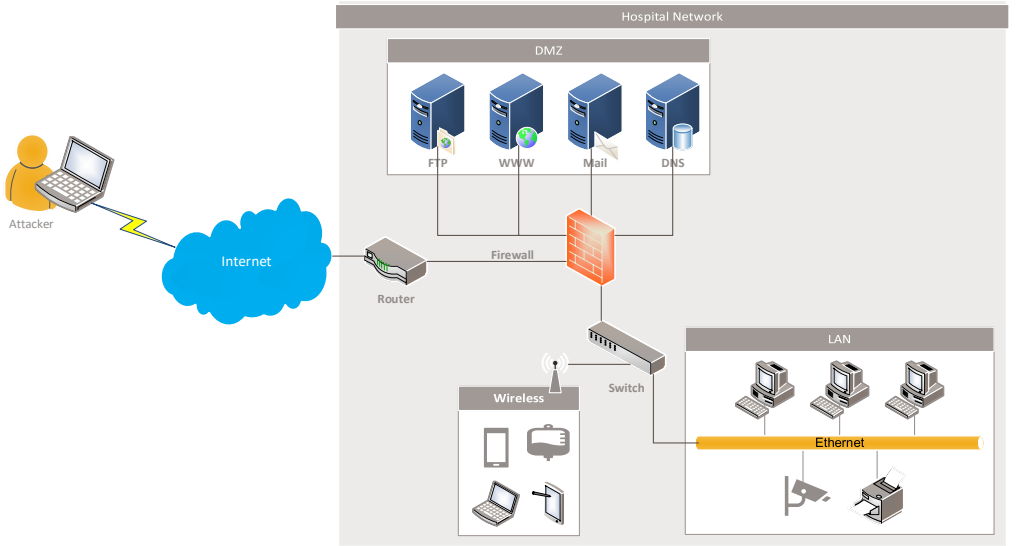
Watering Hole



Man In the Middle



Cross-site scripting (XSS)



Watering hole attacks

Intelligence gathering->point of entry

1. Attacker profiles victims and the kind of websites they go to.

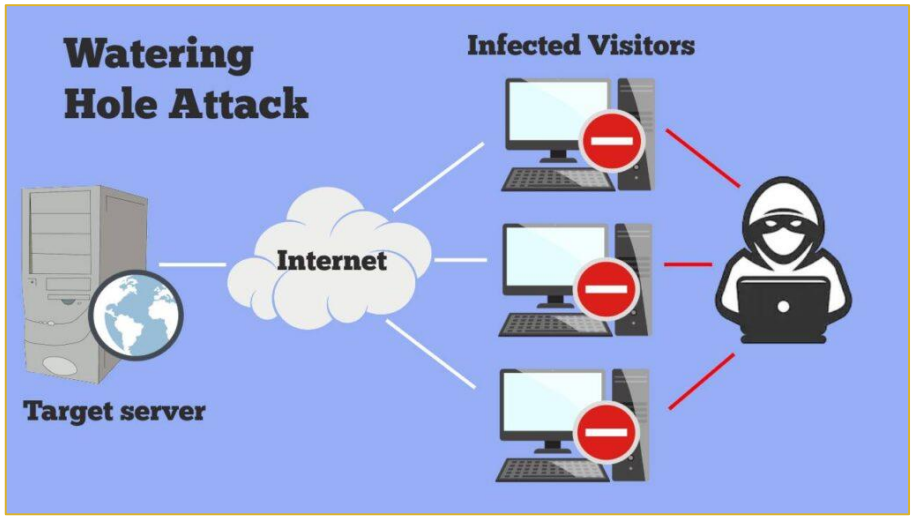
2. Attacker then tests these websites for vulnerabilities.

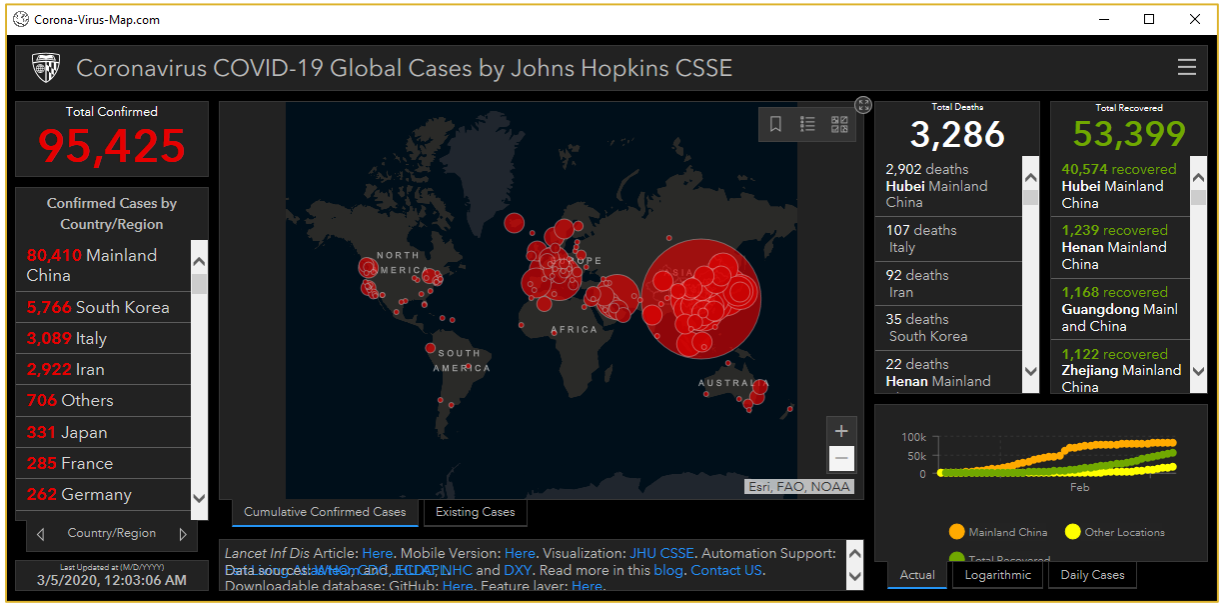
3. When the attacker finds a website that he can compromise, he injects JavaScript or HTML, redirecting the victim to a separate site that hosts the exploit code for the chosen vulnerability.

4. The compromised website is now "waiting" to infect the profiled victim with a zero-day exploit, just like a lion waiting at a watering hole.

Watering hole -> malware

Browser-based attacks affect healthcare to a higher degree because the industry continues to rely on Internet Explorer as the default browser

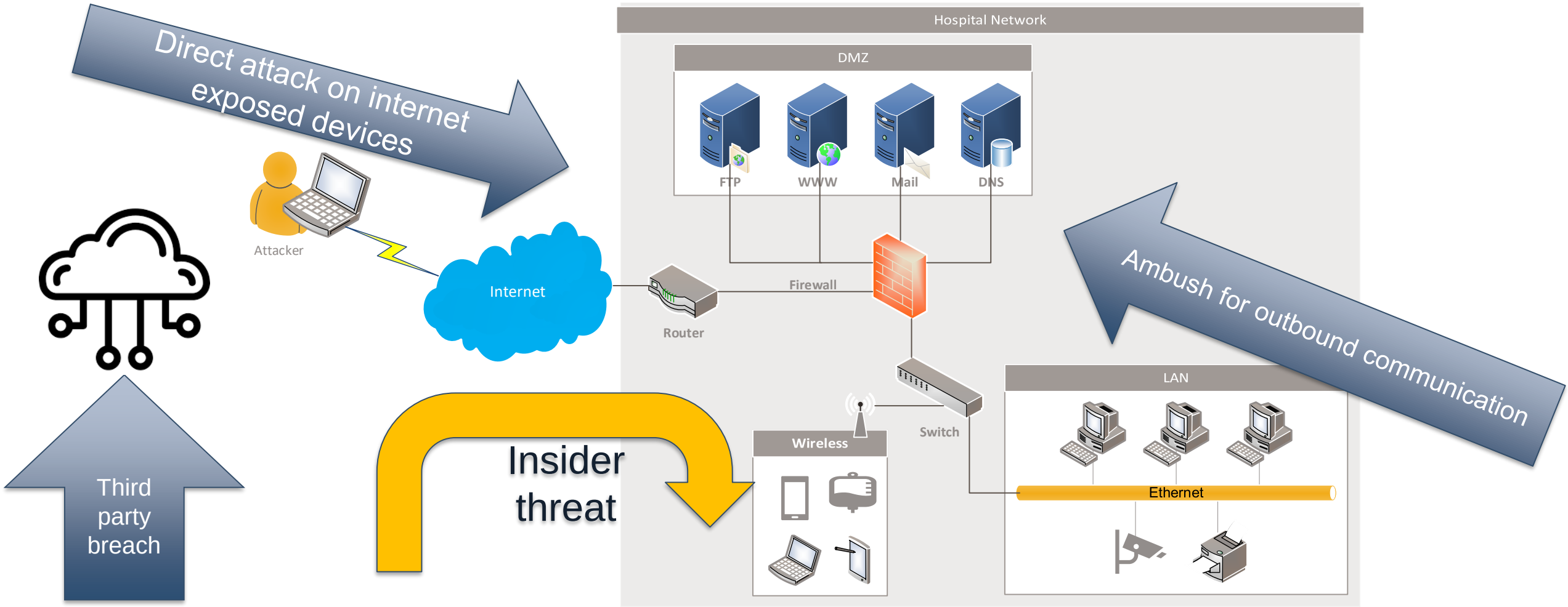




A coronavirus map hiding malicious downloader of a Malware

Points of entry

How the attacker can infiltrate your organization



Insider/physical threat

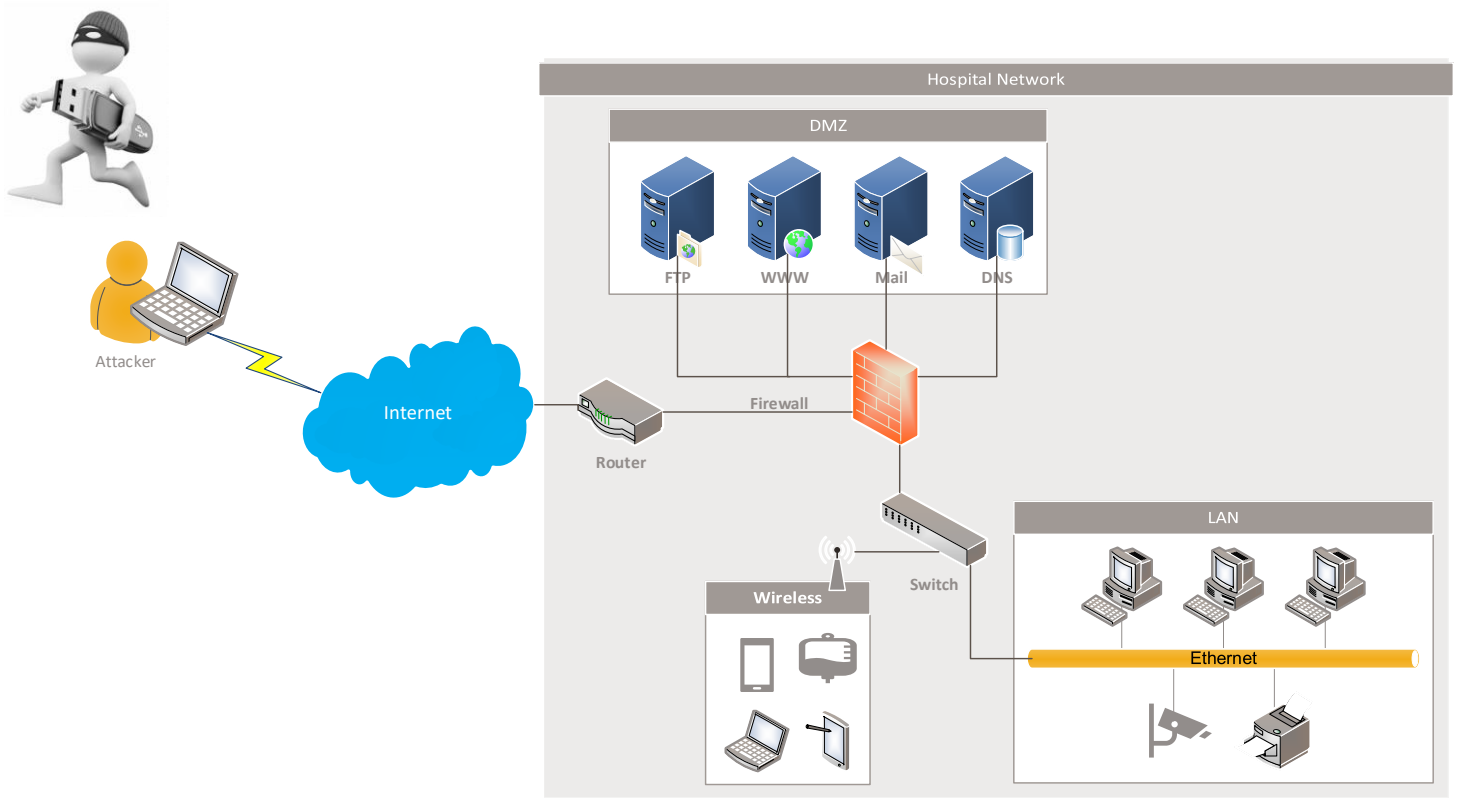
Healthcare attacks common use cases

Computer Theft

Wireless Hijacking

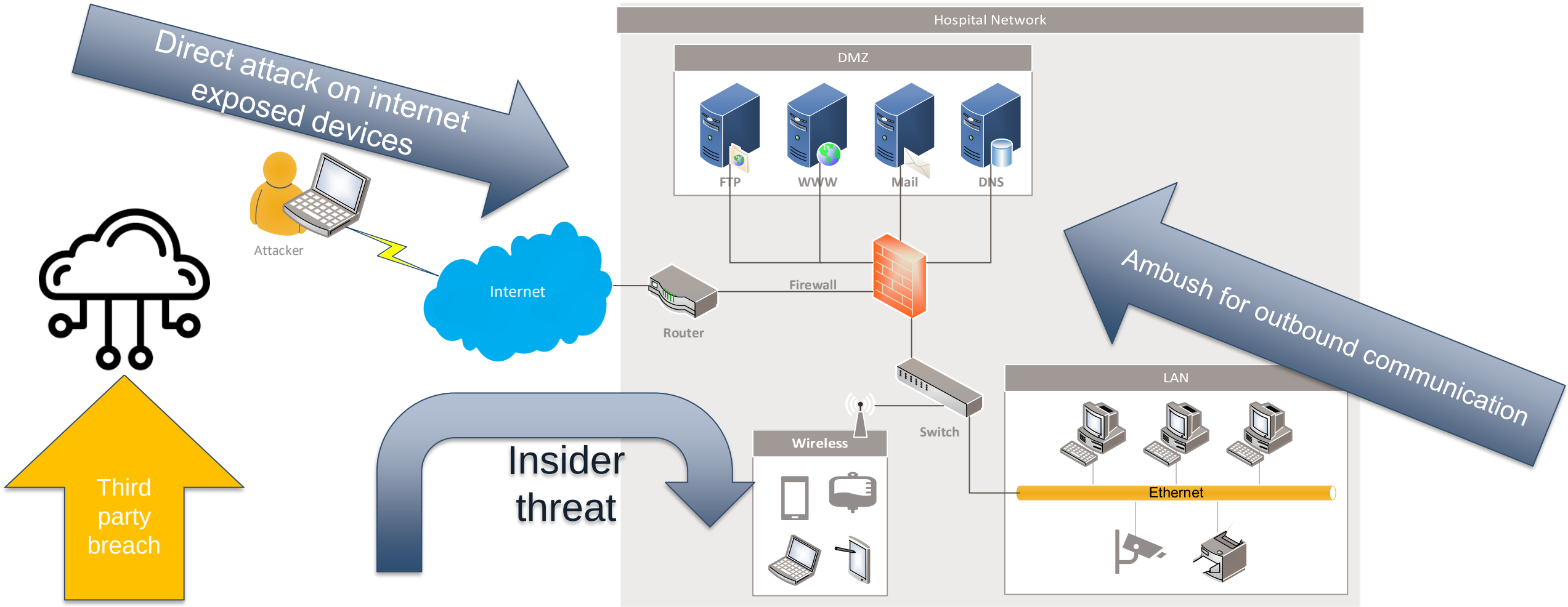
Privilege Abuse

Personal Device Malware



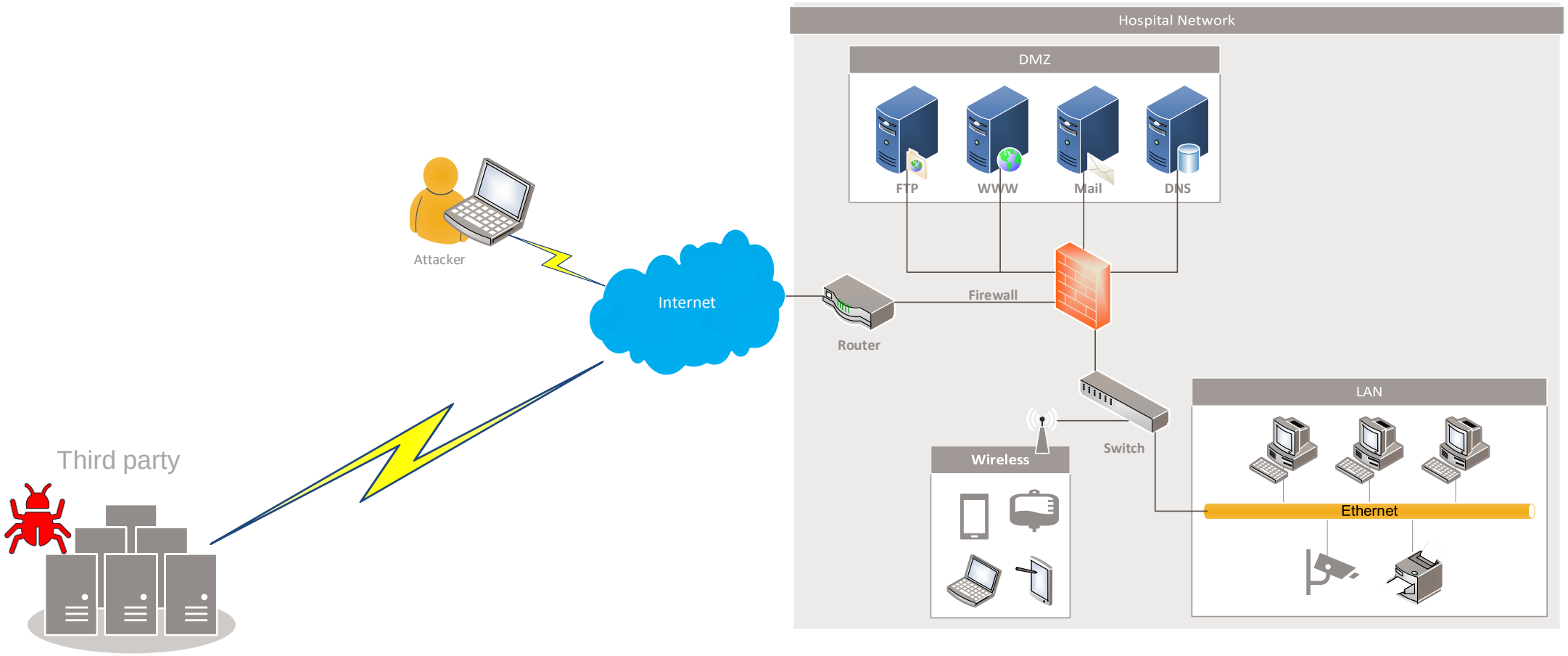
Points of entry

How the attacker can infiltrate your organization



Third party breach

Healthcare attacks common use cases



Third party breach

Healthcare attacks common use cases

User

Pass ‘ or 1=1--

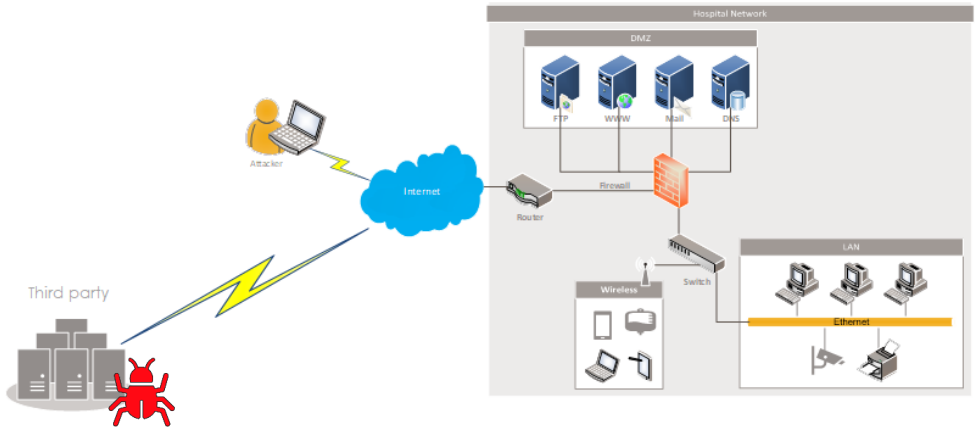
SQL Injection

Vulnerabilities Exploitation

Password Attack

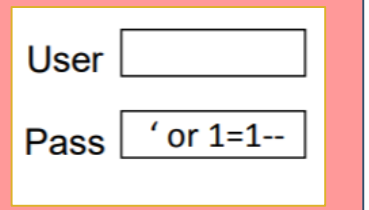
Malware

Phishing



Third party breach

Healthcare attacks common use cases



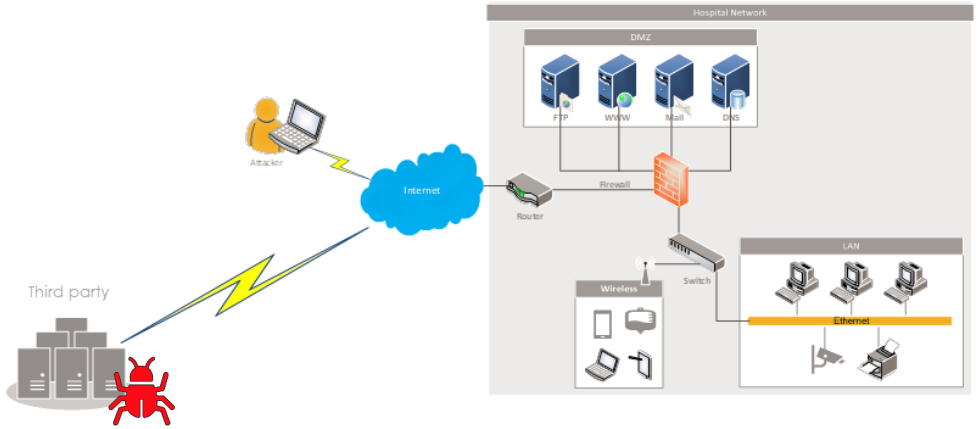
SQL Injection

Vulnerabilities Exploitation

Password Attack

Malware

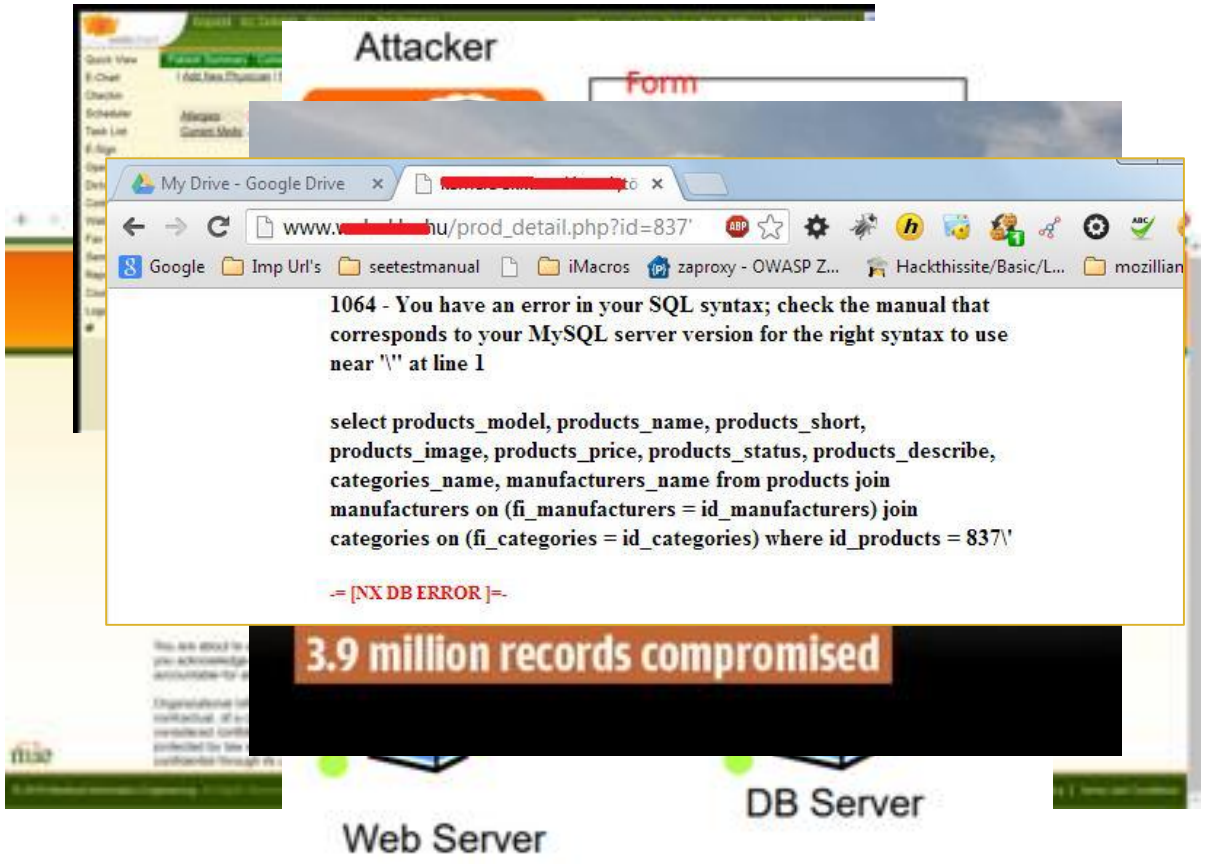
Phishing



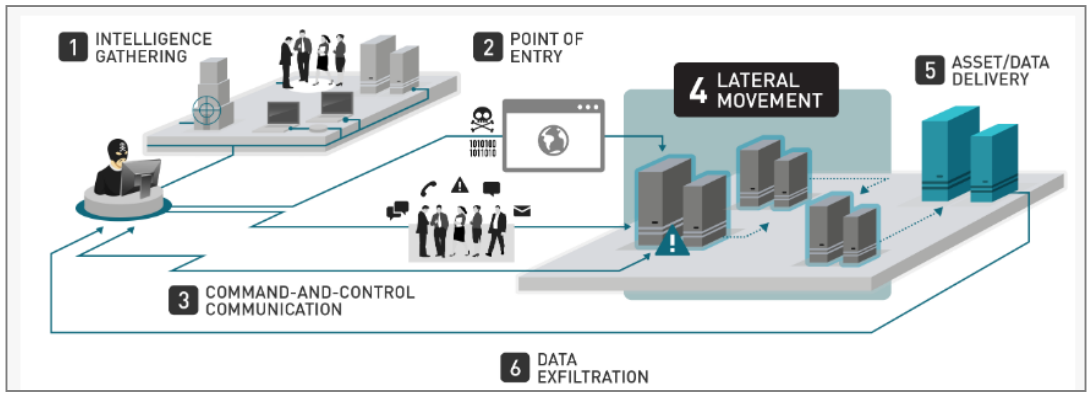
Third party breach - WebChart EMR application

Password attack -> SQL injection -> data exfiltration

- Medical Informatics Engineering, an electronic health records software firm, stored **patient data** in its **WebChart web app**
- Cyber hackers gained access to the web app **remotely by logging in with easily-guessed credentials (User: “tester”, Password: “tester”)**
- The "tester" user did not have privileged access, but did allow the attacker to submit a continuous string of queries, known as a **SQL injection attack**, throughout the database as an authorized user
- The queries returned **error messages** that gave the intruder valuable insight into the **database structure**
- The intruder used information gained from the SQL error messages to access the "checkout" user, which had **administrative privileges**
- The "checkout" user was used to access and **exfiltrate patient records**

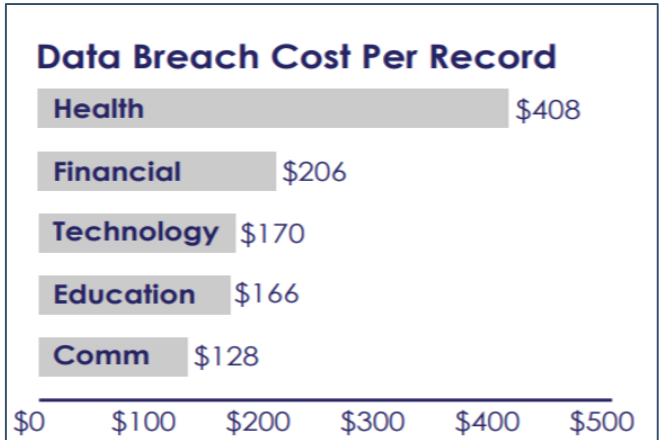


Any questions/comments so far?



Key challenges in balancing the resources with digital transformation and cyber resiliency

Complexity | Value of Healthcare Record | Increasing Threats



The value of healthcare data

Rising Complexity & Connectivity

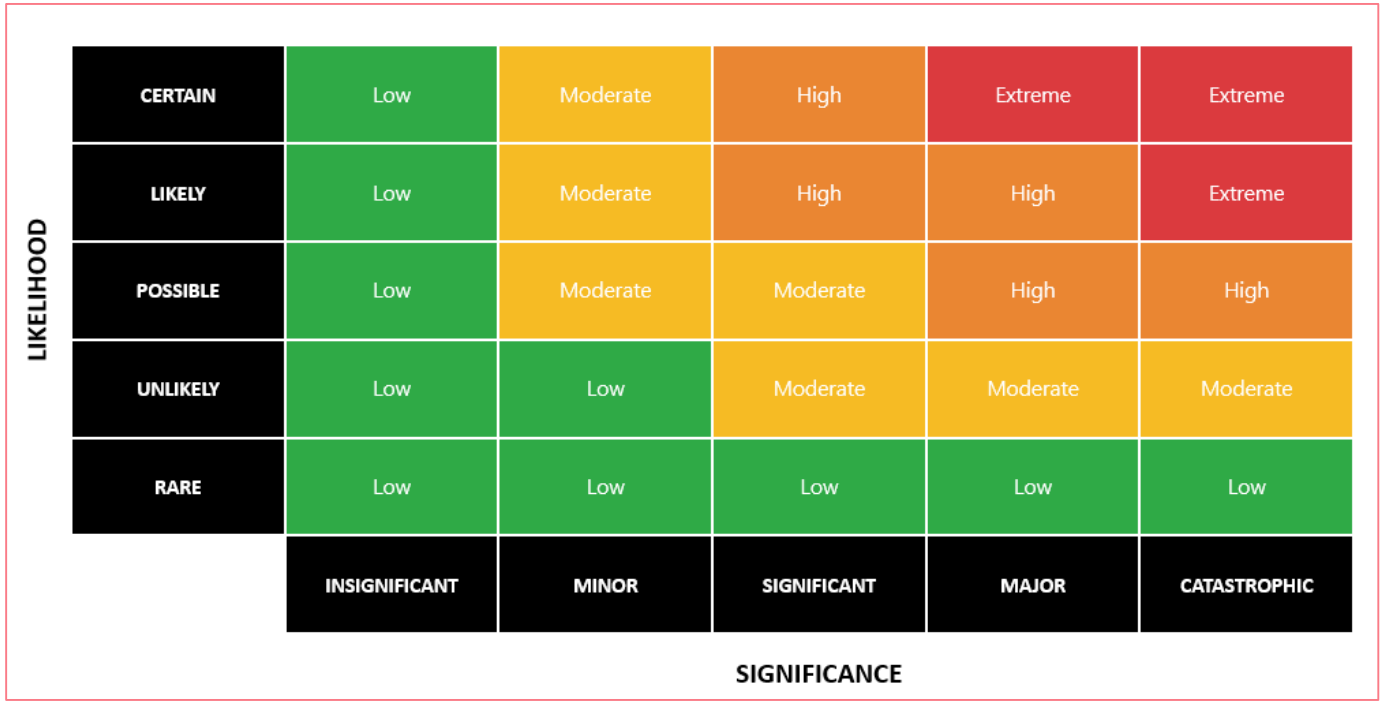
Challenges – Privacy and Cybersecurity

- COVID-19 created significant financial stress
- Crisis required companies to expediently rollout Telehealth program
- Regulators helped to allow several point to point technologies
- Office for Civil Rights (OCR) has published several clarifications and some waivers
- Number of cyber threat actors and attacks continue to increase
- Companies have a business/regulatory need to exchange information
- Retention of cybersecurity and technical resources

Healthcare organizations must address defensive controls while building a strategic program for privacy and cybersecurity

Risks prioritization and remediation

- Resources are limited – have to prioritize critical risks and initiatives
- Conduct ongoing risk assessments and compliance reviews
- Communicate to the operations and leadership teams
- Identify critical infrastructure/crown jewels systems
  - determine a minimum operational security baseline
  - segmentation to minimize the exposure and loss of data (easier said than done)



Practical recommendations and best practices (people | process | technology)

Opportunities for improvement

- Time to establish a robust and meaningful risk management program across the organization
- Review existing security infrastructure and technologies
  - Potential consolidation/integration opportunities
  - Evaluate operational maturity and metrics
  - Transparent communication to the leadership team
- Evaluate critical third-party vendors and their risk management program
  - Business resilience maturity review
  - Review of offshore operations, access, and storage
- Bring visibility to ongoing threats, vulnerabilities, and remediation
  - More challenges for providers with medical devices/technologies
- Security Incidents and breaches
  - Perform thorough and honest investigation
  - Leverage incidents to create continuous improvement

Opportunities for improvement (contd…)

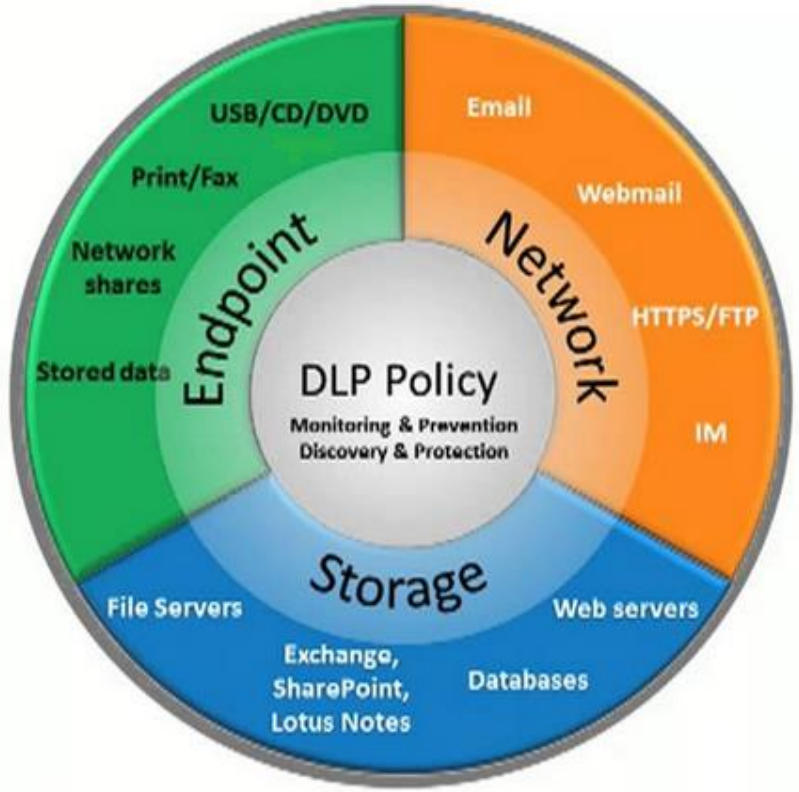
- Develop risk escalation process and matrix/protocol for risk acceptance
  - Executive leadership and Board members should have visibility and understand risks
- Legacy applications – develop a strategy and a roadmap
  - Archiving legacy data | Applying mitigating controls | Minimizing data exposure
- Review of data retention requirements (minimize exposure)
- Security Analytics – quick detection and containment of security incidents
  - Logging, auditing, and monitoring
  - Leverage Security Incident and Event Management (SIEM) and security infrastructure tools to the fullest advantage
- Collaborate and exchange best practices with Healthcare systems in your community
  - Networking with CISOs, Privacy, Security, Legal and Compliance leaders

Data Access | Data Governance | Data Loss Prevention

Data Governance

- Establish a multi-disciplinary group with Clinical, IT, Privacy, Cybersecurity, Compliance, Legal and Operations
- Follow your data – understanding of your data sources, data flows, and review of access is paramount
  - Minimum necessary privileges
  - Periodic access reviews
  - Retention requirements
- Rigorous reviews of external data flows, establishing consistency and transparency, and training of business leaders
- Partners/Business Associates – access from offshore locations and storage of data in offshore facilities
  - Establish quarterly business reviews and annual attestations to ensure accountability

Data Loss Prevention program (technology is just one part)



COVID-19 and Business Resilience

- Healthcare providers operate with poor maturity in handling business continuity, IT disaster recovery, and emergency management
  - COVID crisis presents an opportunity to revamp the entire program

- Consumers/Patients | Workforce | Partners/Business Associates

- Communication strategy/platform specific to pandemic crisis

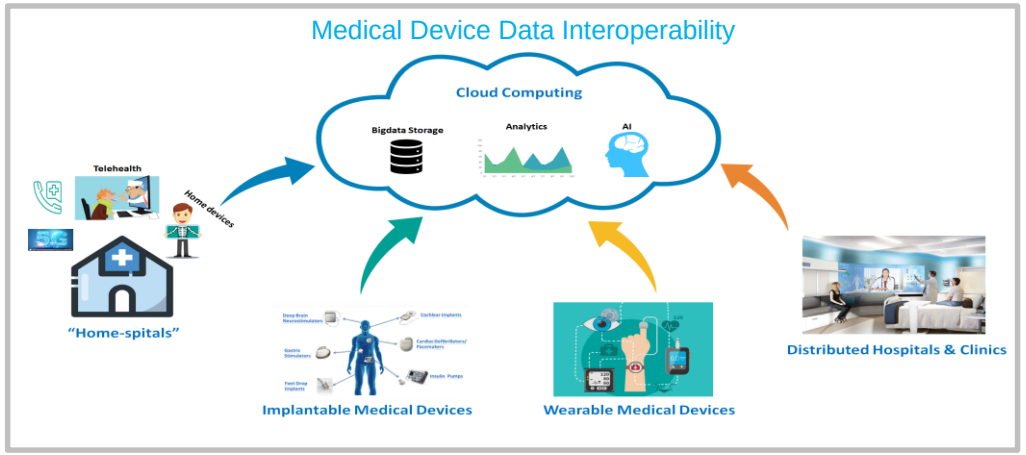
- COVID-19 and the future of work strategies – lessons learned from Tech companies
  - Re-evaluate policies for Work from Home
  - Flexibility with Staffing and Hours
  - Remote Collaboration Technologies
  - Train employees to build productivity
  - Manage mobile and personal devices

What is a Business Continuity/Disaster Recovery (BC/DR) plan?

Spare tire	BC/DR plan
Minimum maintenance	
Check and inflate whenever normal tires are inflated.	Test backups monthly. Test full plan every year.
Replaced at first signs of dry rot. Or every 6-10 years depending on tire.	Revise following major changes in application or infrastructure. Typically 3-5 years.
Consequences	
Spare tire may fail when you need it most, resulting in towing fees, property damage, injury, or death.	DR/BC Plan may fail when you need it most resulting in data loss, unacceptable downtime, fines, and impact to patient care.

Medical Device Security

- Cybersecurity of medical device hardware and software is a patient care concern
  - Traditional focus has been on safety and efficacy for one patient at a time
  - Cyber compromise can impact many patients (Ex: tens of thousands infusion pumps recalled due to vulnerability)
- Need waivers and mandate for cybersecurity tool interoperability
  - Antivirus, endpoint integrity, encryption, data sanitization
  - Typical medical device OSs support all major tools
  - FDA device review / clearance process excludes out cyber tools
  - Vendors unable / unwilling to allow many cyber tools
  - MDS2 verification
- New approaches:
  - Automatic identification & classification
  - Flow visibility and behavioral anomaly detection
  - Context aware micro/macro-segmentation



Brainstorm – practical recommendations and best practices

(People | Process | Technology)

Communication strategies to the leadership
-
Threats, vulnerabilities, and organization's preparedness

Thank You!

Ram Ramadoss
System Senior Vice President, Privacy, Information Security and EHR Compliance

Phone: +1 (720) 624-9613
Ramramadoss@catholichealth.net

Ido Geffen
VP Product & Customer Success

Phone: +1 (646) 860-5452 / +972 (55) 559-4126
Ido@CyberMDX.com

Closing

For more cybersecurity information and best practices, be sure to check out the 405(d) publication titled:

Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP)

The publication details the top five threats facing the healthcare industry and the top 10 practices to mitigate. Read the entire publication on our website: www.phe.gov/405d.

Next 405(d) Spotlight Webinar:

August: Date and Topic TBD; Invites will go out in early July!

This webinar is for information purposes only and aims to broaden awareness and align healthcare security approaches. The topics chosen are developed by a different 405(d) task group member each iteration and do not reflect the views of HHS as a whole. All task group members have been invited to contribute this webinar series.

Thank you for joining us!

Visit us at: www.phe.gov/405d

Contact us at: CISA405d@hhs.gov