HEALTHCARE SECURITY: THE BIRD'S EYE VIEW

Presented by Inherent Security

INHERENT SECURITY

Founded in 2018

Specialize in Healthcare

HIPAA
Cyber Program Development
NIST Special Publications

Involvement

Chair - Health Tech Committee NVTC
Contributor - CISA 405(d) Cyber Task Force HHS
Board Member - MIT Enterprise Forum DC & Baltimore

FOUNDER

Larry Trotter II

CEHv7, ESCA, GCIA, ITIL, CISM,

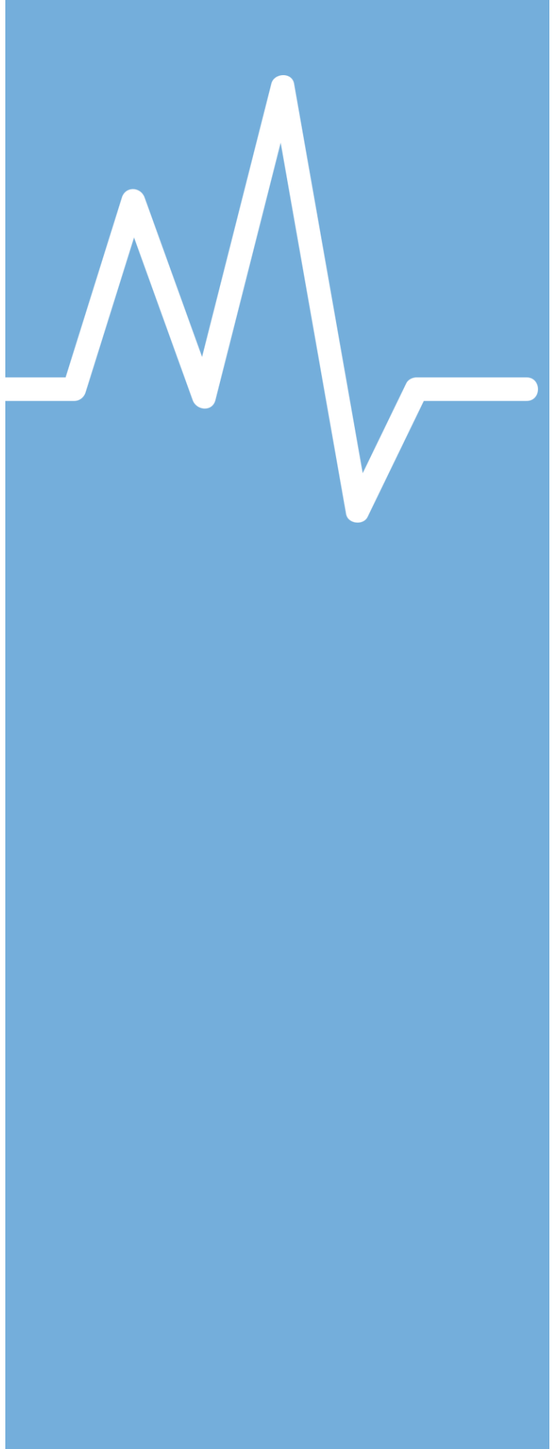
Why is Healthcare Data Valuable?

Oil is old News!

Transformative technology – leveraging data and technology to enhance human well-being

Data monetization - Providers, EHR vendors, and device manufactures are rethinking their data strategies to include direct monetization.

Example: A recent agreement between GlaxoSmithKline (GSK) and 23andMe is the first publicly disclosed example of direct monetization. Although it is being promoted as a collaborative use of the genetic data in 23andMe's possession, many have concluded that the data was sold to a high bidder. In the agreement, GSK invests $300M in 23andMe in exchange for access to the genetic information of its five million customers, with the goal of accelerating treatments and cures.



Healthcare Data is Vulnerable.

Moves among patients, hospitals, EHR, clinics, devices, etc.

Motion presents danger i.e. vulnerabilities

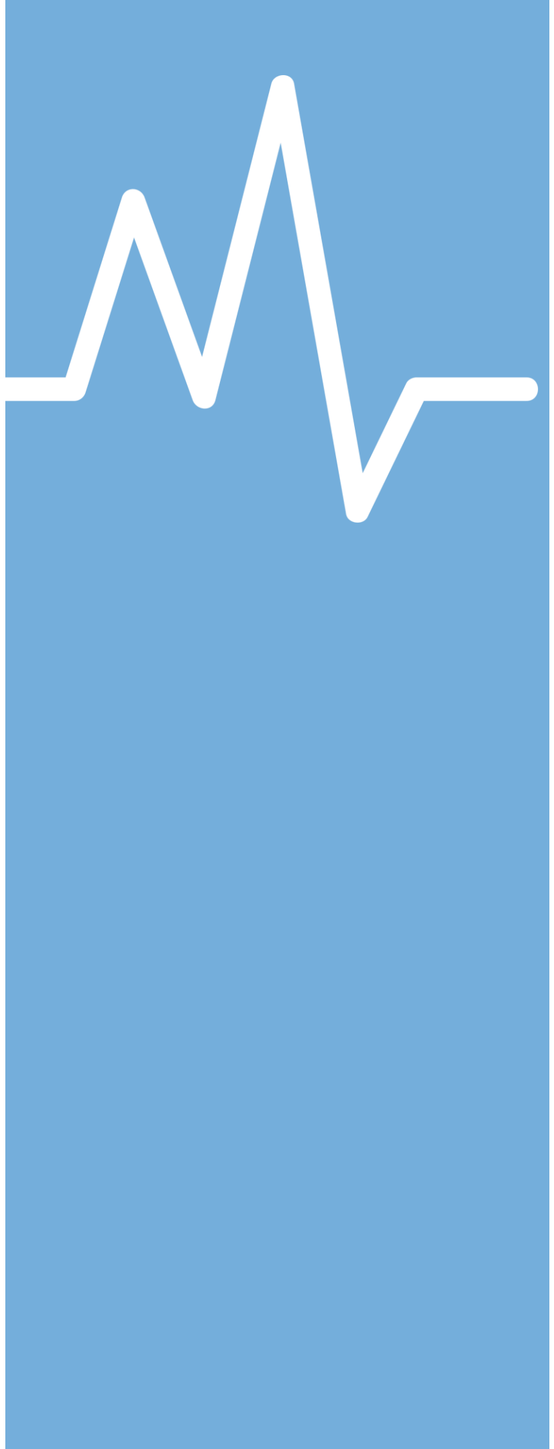
Privacy! It is hard to regulate

Risk Assessments are not performed

Priority Issues with cybersecurity

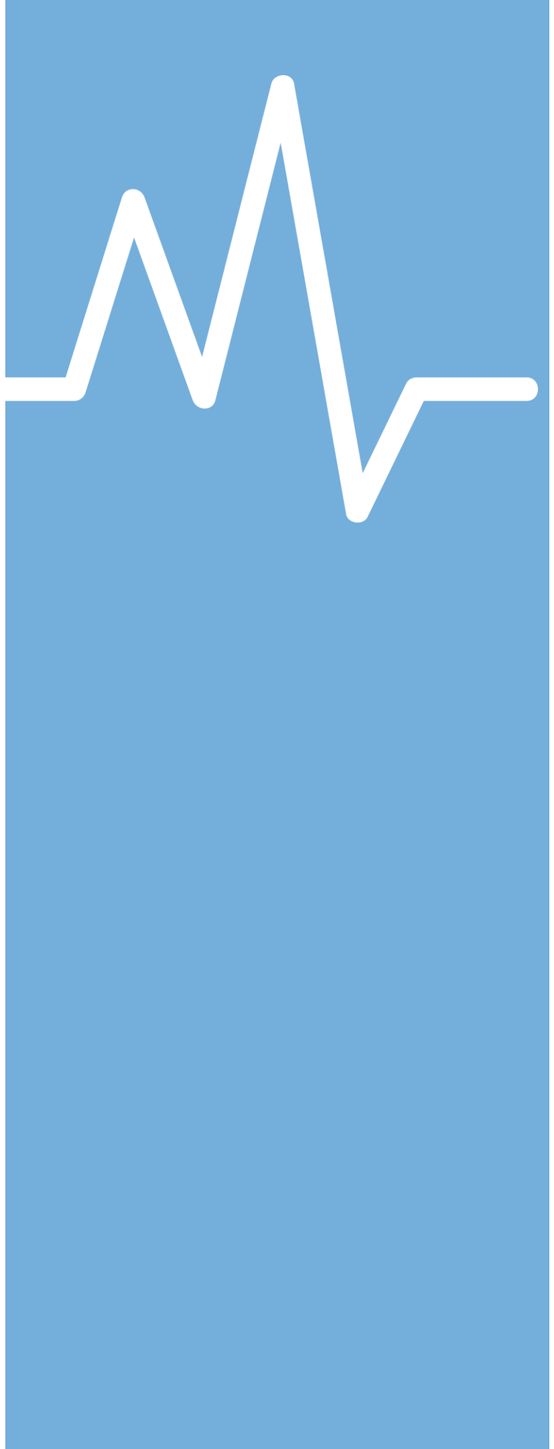
Healthcare has the most breaches compared to any other industry; account for 25% of the pie

Compromised Patient accounts trippled between 2017 and 2018



HIMSS19 Top 8 Tech Healthcare Adoption Trends

1. BI and FI Analysis
2. Artificial Intelligence
3. Interoperability and HIE
4. Telehealth
5. Consumer and Connected Health
6. Analytics Tech Upgrades
7. Cybersecurity
8. Patient Portals



“

When health care providers have access to complete and accurate information, patients receive better medical care.

ONC

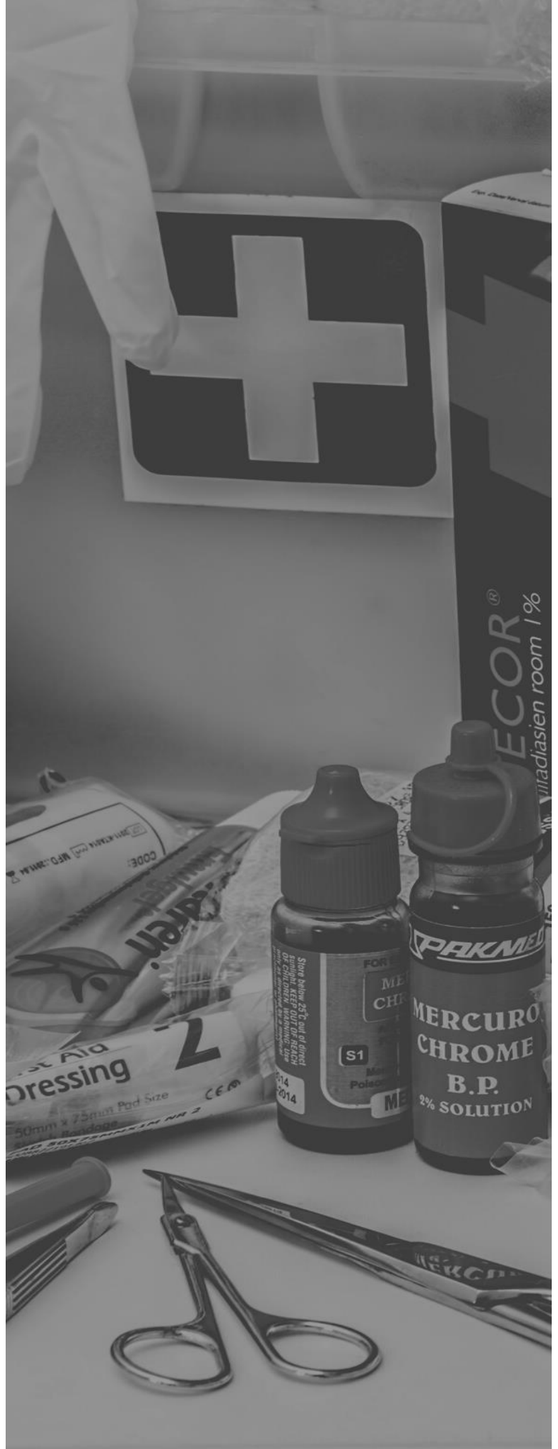
”

Medical Image and Data Leaks...

Sept 17, 2019

" Hundreds of computer servers worldwide that store patient X-rays and MRIs are so insecure that anyone with a web browser or a few lines of computer code can view patient records."

- 5 servers in Germany and 187 in the U.S. made patients' records available without a password
- More than 5 million patients data sets affected in the U.S. and millions more around the world
- A person could use free software programs — or just a typical web browser
- Servers not password protected or missing basic security precautions
- MobilexUSA displayed the names of more than a million patients — all by typing in a simple data query. Dates of birth, doctors and procedures were also included
- Experts say it's hard to pinpoint who's to blame for the failure to protect the privacy of medical images?
- Most of the cases of unprotected data found involved independent radiologists, medical imaging centers or archiving services



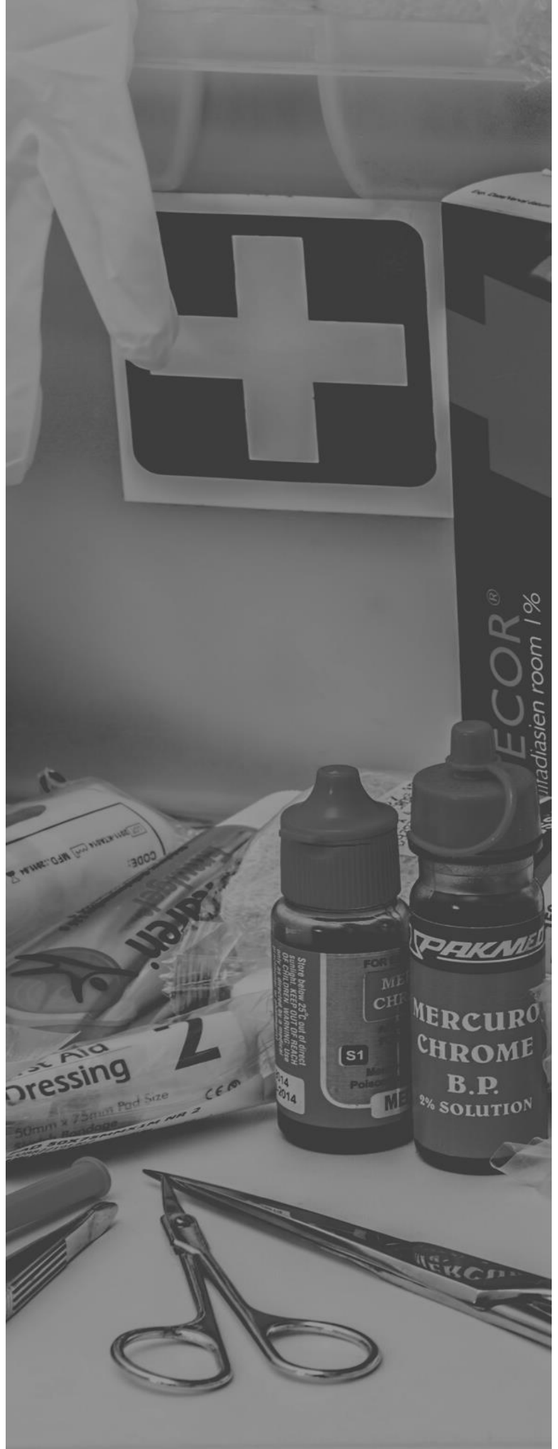
Help is out there!

Published Sept 16, 2019 NIST SP 1800-24 Securing Picture Archiving and Communication System (PACS) - Draft

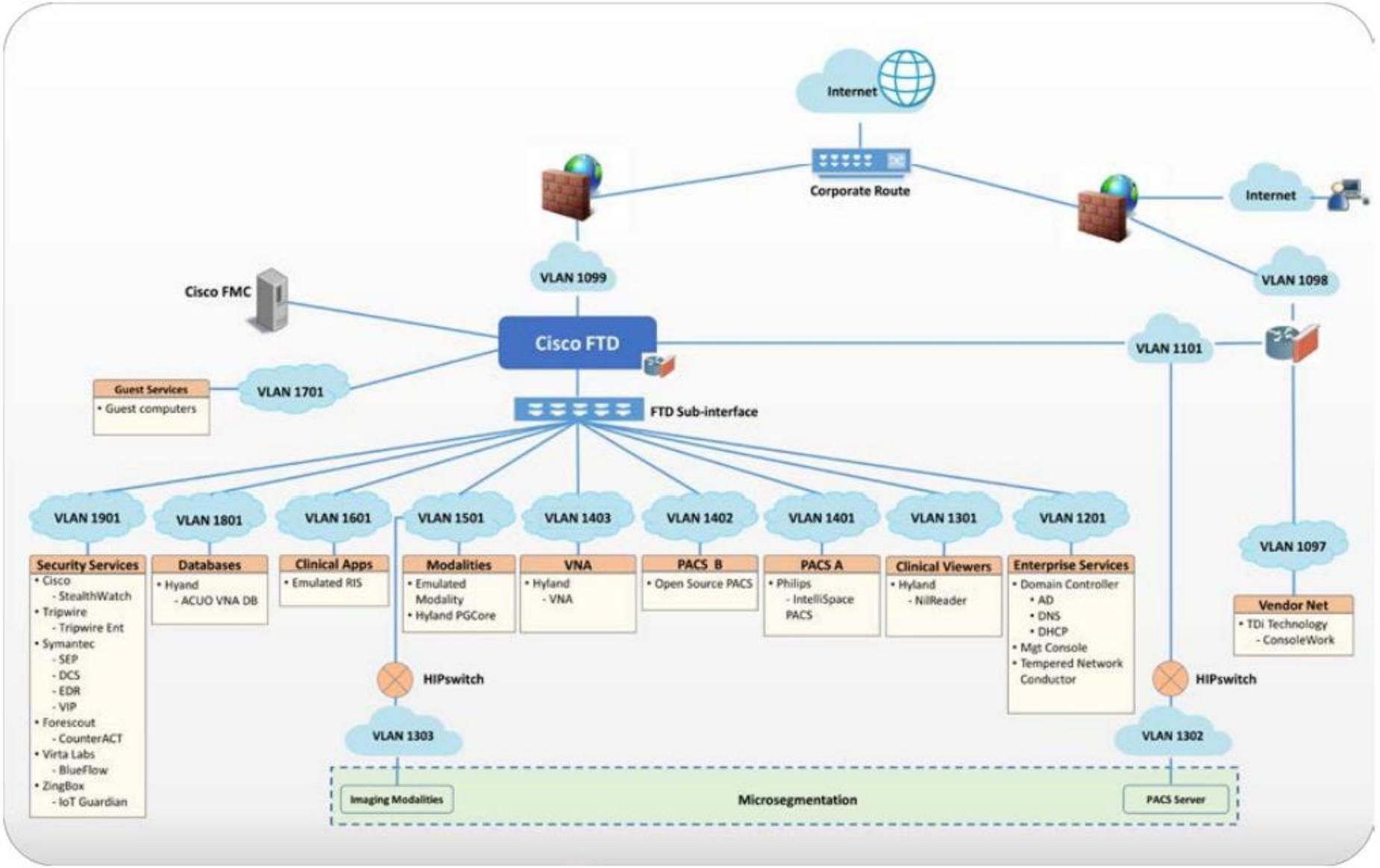
NIST used a holistic risk management approach that includes medical device asset management, augmenting enterprise security controls and leveraging behavioral analytic tools for near real time threat and vulnerability management in conjunction with managed security solution providers.

This practice guide demonstrates: a defense-in-depth solution, including network zoning that allows for more granular control:

- network traffic flow and communication limitation capabilities to the minimum necessary to support business function
- access control mechanisms that include multi-factor authentication for care providers, certificate-based authentication for imaging devices and clinical systems, and mechanisms that limit vendor remote support to medical imaging components



NIST SP 1800-24 Securing Picture Archiving and Communication System (PACS) - Draft



IoT Devices

Ecosystem of inter-connected computing devices that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

Telehealth

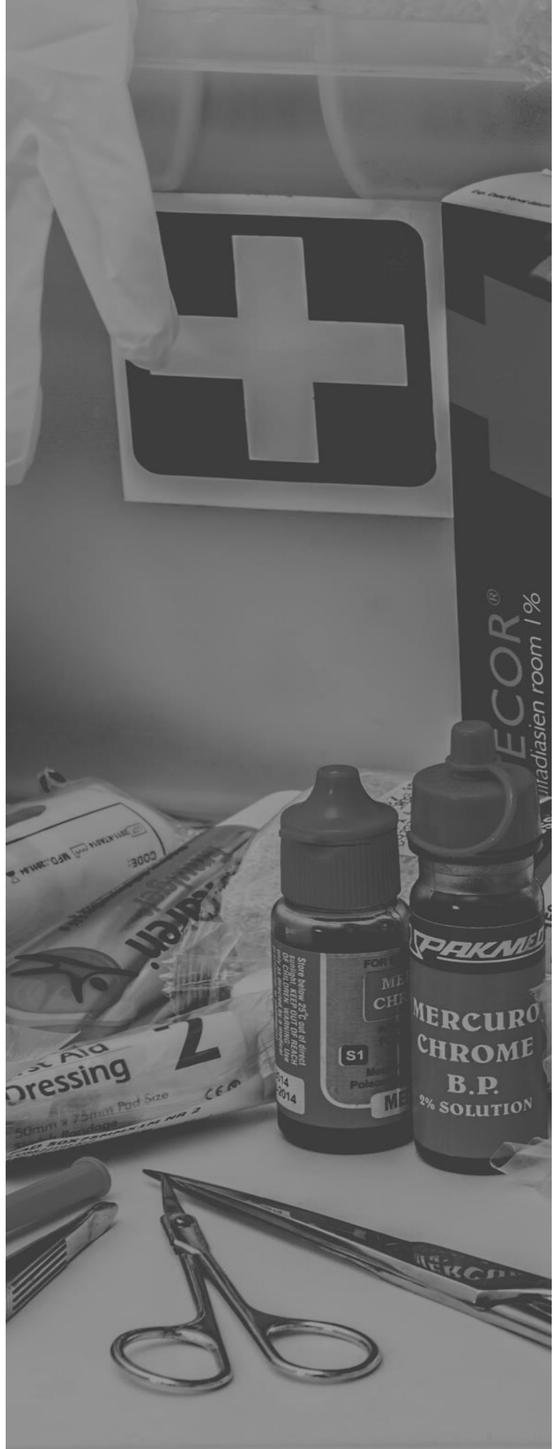
The use of electronic information and telecommunication technologies to support long-distance clinical health care, patient and professional health-related education, public health and health administration

Smart Hospitals

Smart hospitals rely on optimized and automated processes, built on the IoT and on the big data revolution which combines connected devices with cloud computing, big data analytics and artificial intelligence (AI).

Smart Pills

"Ingestible Sensors“ These pill-sized sensors monitor the medication in the patient’s body and warns if it detects any irregularities



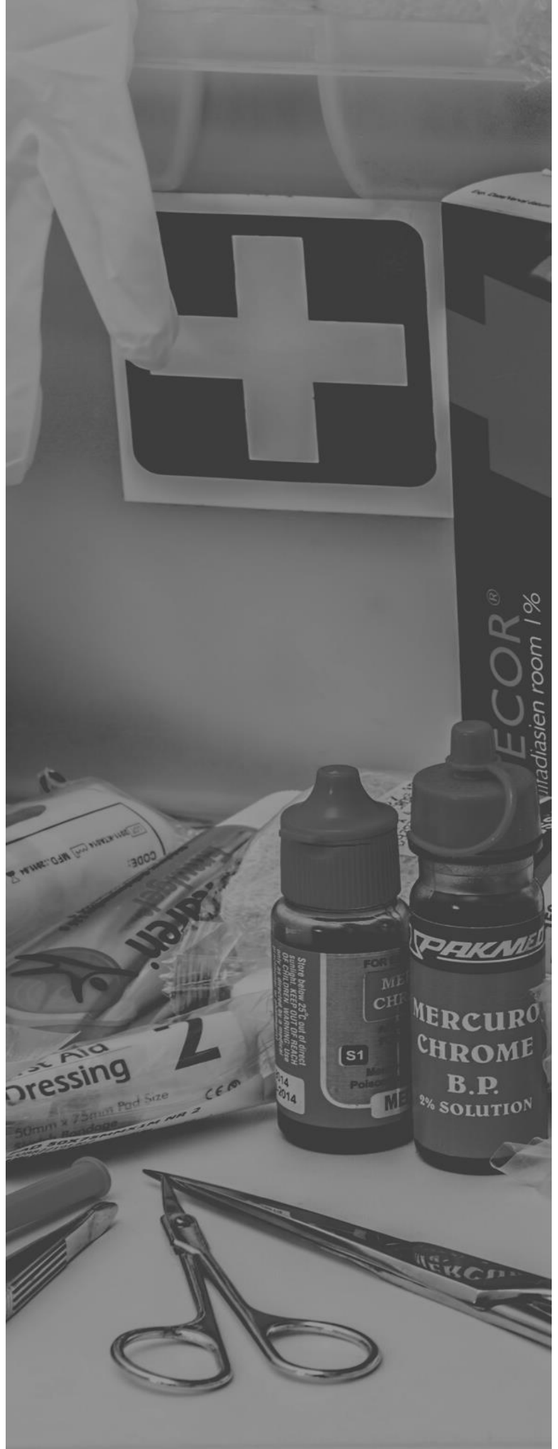
IoT Devices

Benefits

- Remote monitoring
- Efficient coordination of medical care (EHR)
- Disease Monitoring
- Smarter Hospitals (Improving Staff and Patient experience)
- Reducing Emergency Room Wait Times
- Ensuring the Availability and Accessibility of Critical Equipment
- Enhanced Drug Mgmt

Challenges

- Devices are often built on outdated software and legacy operating systems that leave them vulnerable
- Devices are increasingly collecting and storing vast amounts of data which makes them an attractive target for cyber criminals
- Privacy can be potentially undermined
- Denial of Service (DOS)



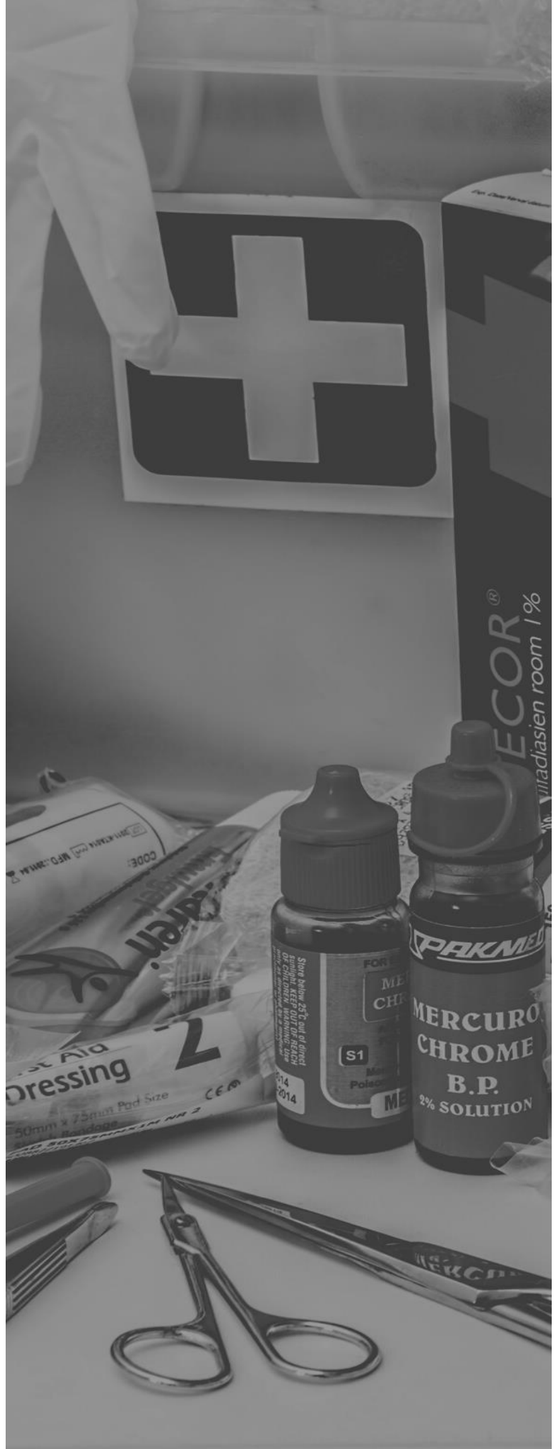
IoT Data Security Concerns?

•82% of healthcare providers that have implemented IoT devices have experienced a cyberattack on at least one of those devices over the course of the past 12 months, according to the Global Connected Industries Cybersecurity Survey from Swedish software company Irdeto.

•Surveyed 700 security leaders from healthcare organizations and firms in the transportation, manufacturing, and IT industries in the United States, United Kingdom, Germany, China, and Japan. Attacks on IoT devices were common across all those industry sectors, but **healthcare organizations** experienced the most cyberattacks out of all industries under study.

Example

In a recent case in Ohio, police were able to obtain a search warrant for a suspect's pacemaker data to be used as evidence in an insurance fraud case. While the search did prove that the suspect had committed insurance fraud, the use of medical data as evidence by law enforcement officers creates a dangerous precedent.



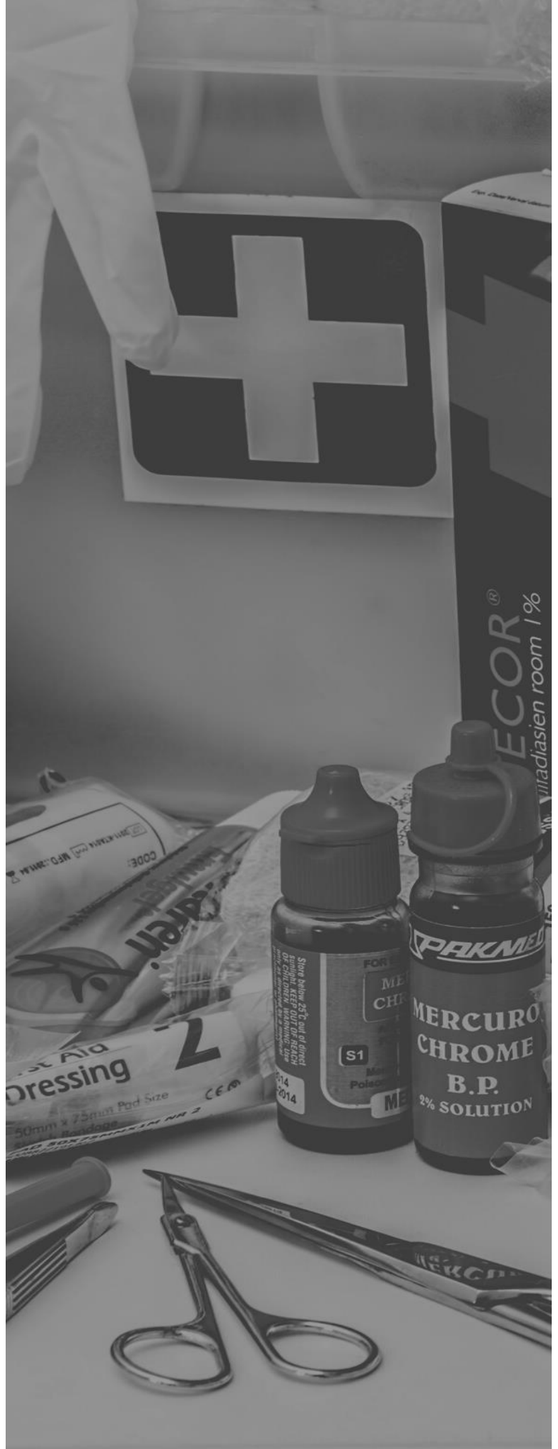
IoT Data Security Concerns?

Sept 09, 2019

•Microsoft found Strontium (Russia) launching attacks in an effort to compromise several commonly used IoT devices, like office printers or VOIP phones, across a wide range of sectors. During the attacks, the hackers leverage their infrastructure to communicate to the external IoT devices and successfully gained initial access to the network of the corporate targets.

•Further investigation into two of the occurrences showed the actors gain access using the devices' **default password** that the organization failed to change. In the third instance, the researchers found the victim had not updated the device with the **latest security patch**.

•Once the actor had successfully established access to the network, a simple network scan to look for other insecure devices allowed them to discover and move across the network in search of higher-privileged accounts that would grant access to higher-value data.

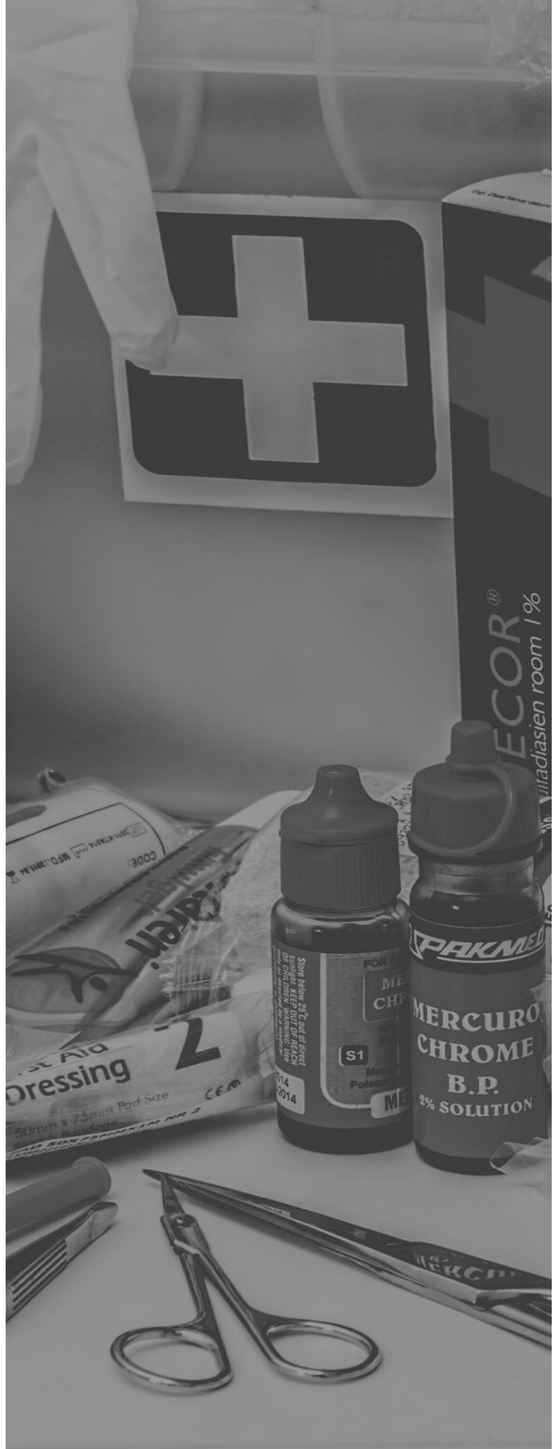


Threat Intelligence: IoT Indicators

HIDDEN HTTPS TUNNELS
the most prevalent method attackers use to hide their command-and-control communications in healthcare networks was through hidden HTTPS tunnels. This traffic represents external communication involving multiple sessions over long periods of time that appear to be normal encrypted web traffic. When attackers hide their command-and-control communications in HTTPS tunnels, it often looks like legitimate traffic.

HIDDEN DNS TUNNELS
The most common method attackers use to hide data ex-filtration
behaviors in healthcare networks was through the use of hidden DNS tunnels. In a hospital, patient data in motion is quite normal due to the sharing of patient records between medical professionals to provide health care as well as the management of medical devices by the device manufacturer

RANSOMWARE AND BOTNET
While many healthcare organizations experienced ransomware attacks in recent years, the report found that ransomware threats were not as prevalent in the second half of 2018.



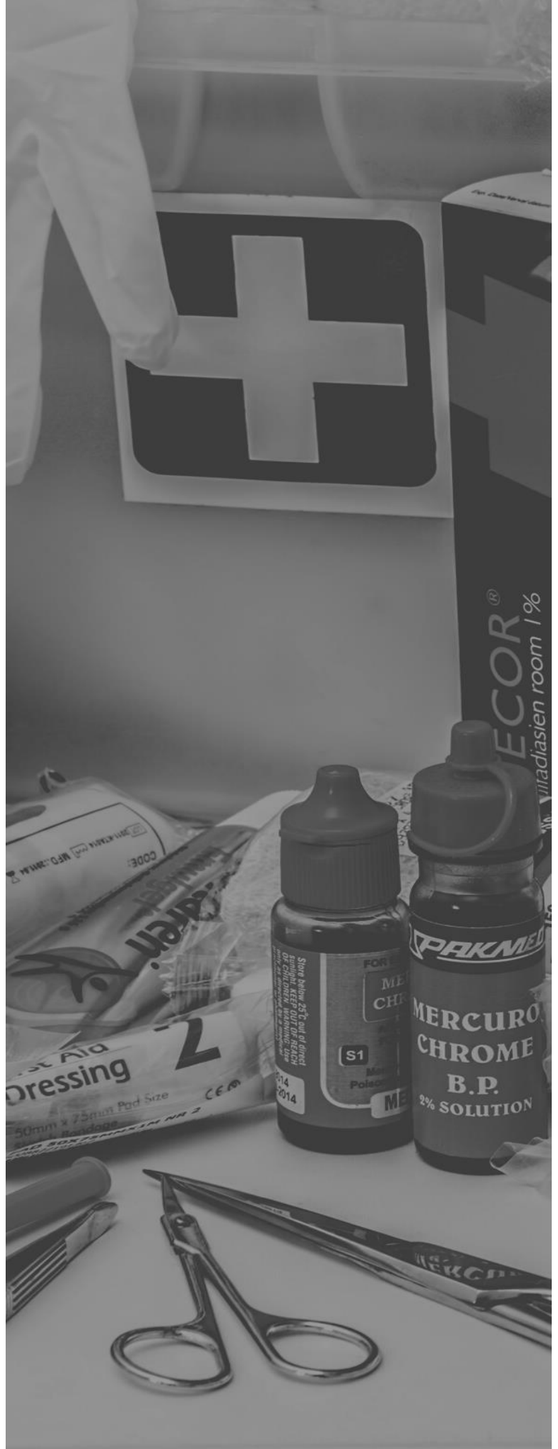
IoT Security Help for Manufactures and Providers

Draft NISTIR 8259 Core Cybersecurity Feature Baseline for Securable IoT Devices: A Starting Point for IoT Device Manufacturers

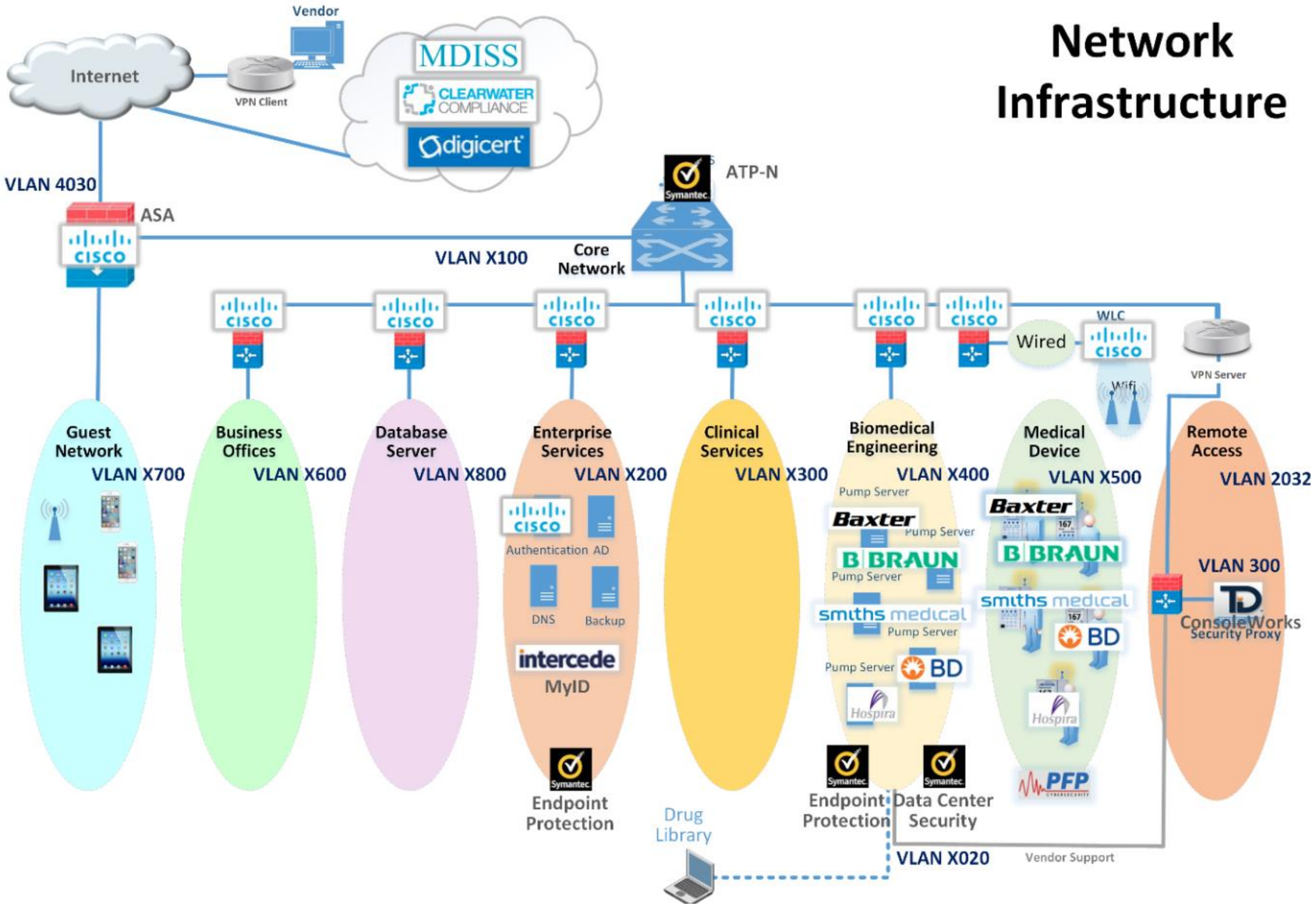
- Device Management
- Configuration
- Network characteristics
- Data Encryption, Backup\Restore, Authentication
- Access Controls

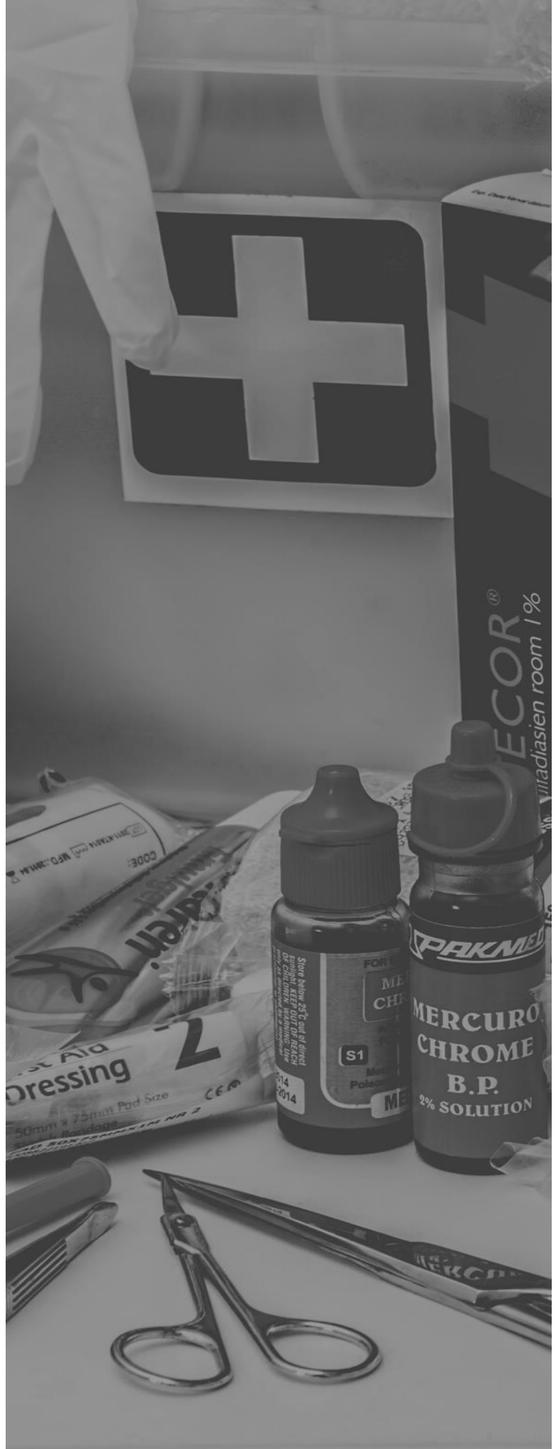
NISTIR 8228 Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks

- Protect device security
- Protect data security
- Protect individuals' privacy



NIST SPECIAL PUBLICATION 1800-8 Securing Wireless Infusion Pumps





Organizational Struggles in Healthcare

Common Themes

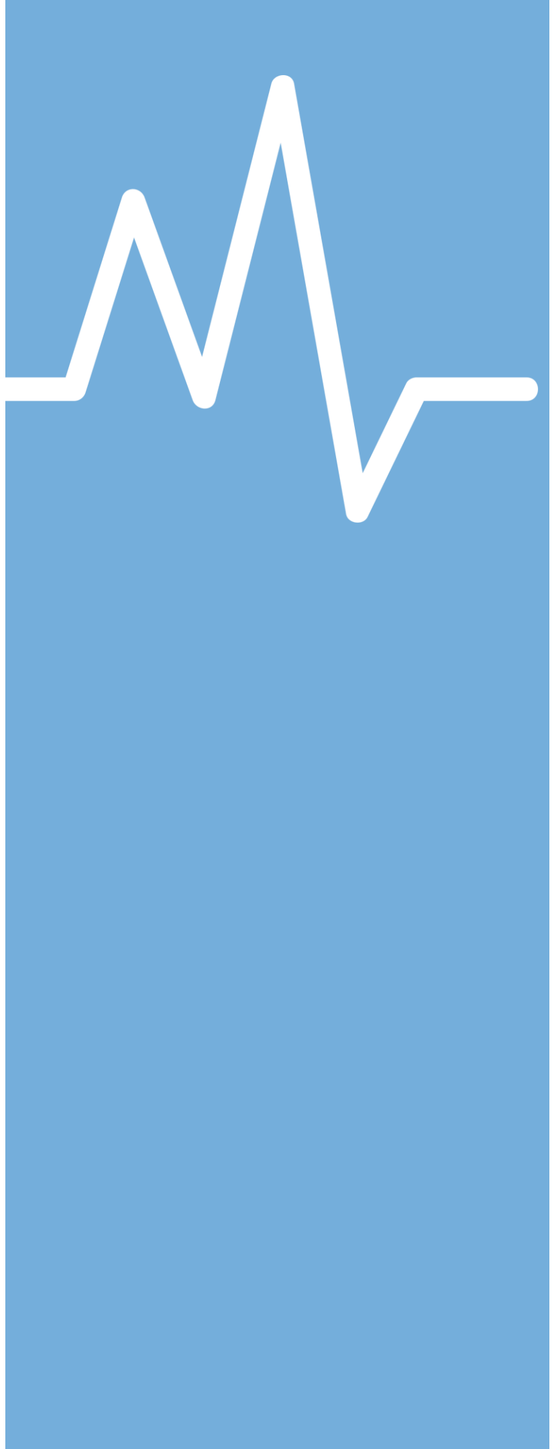
Organizational Structure (Complexity, Centralization, and bureaucracy)
Human Resources (Staff)
Work Nature (Stress and Team Oriented)
Leaders (Knowledge and Skills)
Context (Regulations and programs, Cultural issues)

54% of healthcare associates say their biggest problem is employee negligence in the handling of patient information.

- Security Awareness Training Programs
- HIPAA Training
- System Auditing
- Data Loss Prevention (DLP)

42% of healthcare organizations leave their cybersecurity in the hands of a Vice president or C-level official.

- Separation of Duties
- CISO
- Think Security Operations
- Manage Service Provider



Organizational Struggles

The biggest internal cyber security threats to healthcare are often high-ranking officials and senior staff who have deep access to the system.

61% of organizations cited Senior-level executives as a potential security loophole that can be vulnerable to cyber threats.

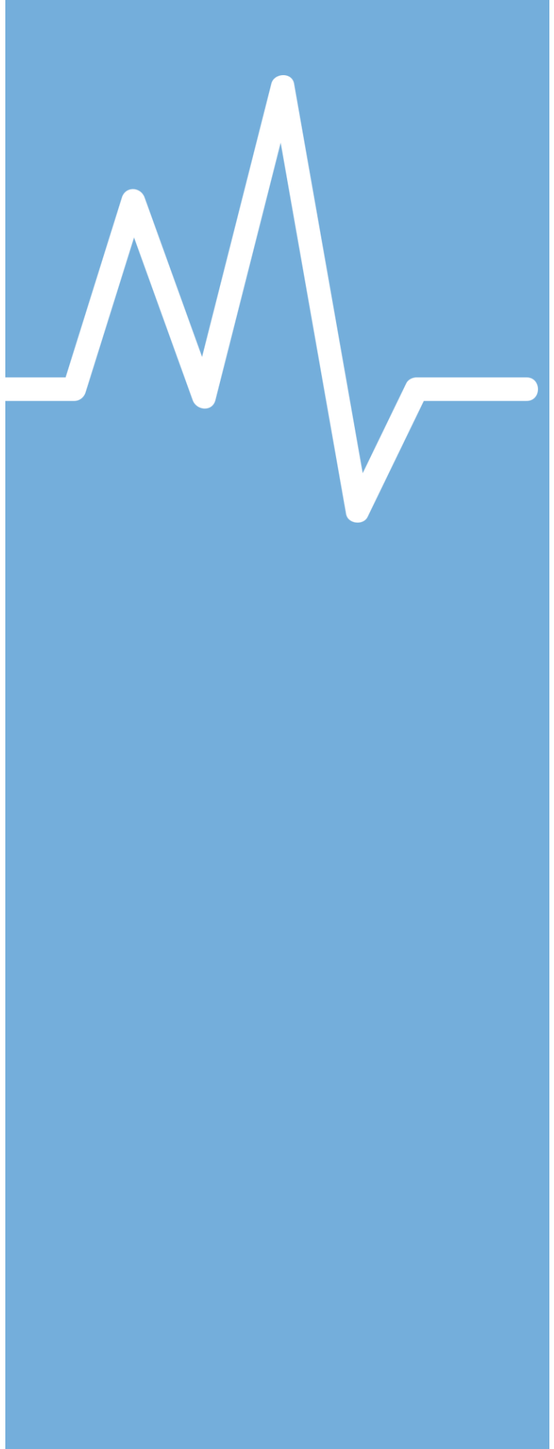
Similarly, privileged users, such as executive managers, contractors, and service providers, are potential targets for hackers and cybercriminals.

- Least Privileged Access
- Security Awareness Training
- Remote Travel Security Measures

Executive Leadership Reporting

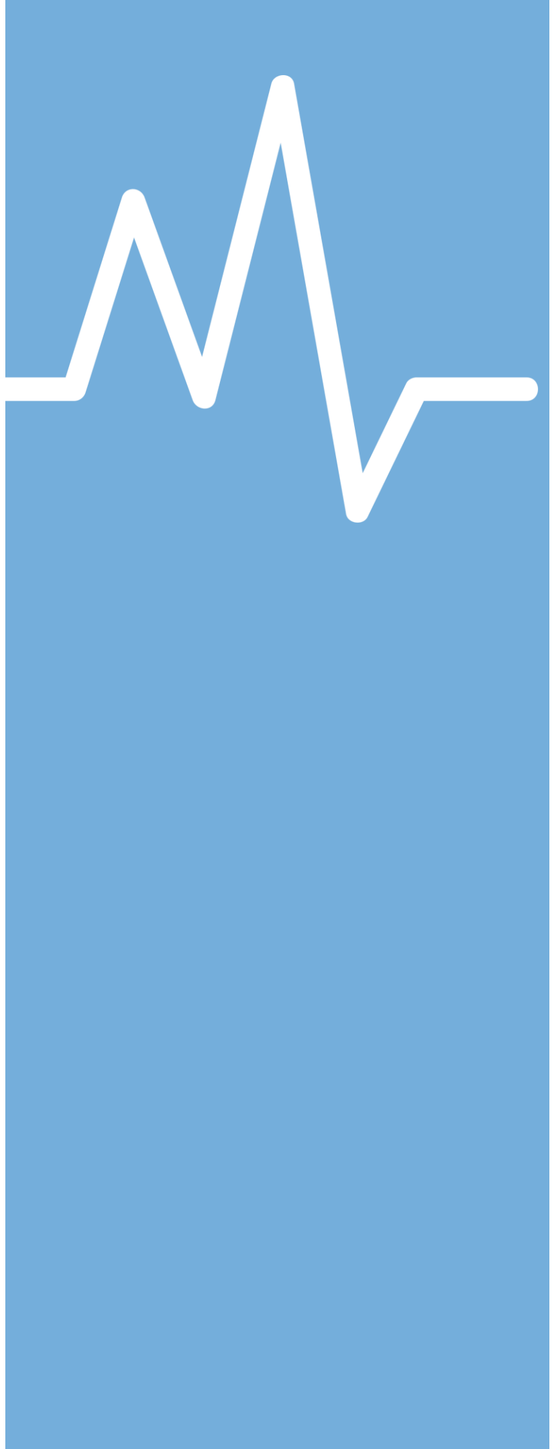
•A HIMSS study show that organizations in which the CISO reported to the CIO experienced 14% more downtime due to cyber-security incidents than those organizations in which the CISO reported to the CEO.

Organizations in which the CISO reported to the CIO reported financial losses 46% higher than when the CISO reported to the CEO.



Organizational Struggle Example

Dr. X, MD, MS, is the CIO of Medical Center. Although his business cards describe him as a CIO, in 1998 he was given the title CMIO. In reality, he works as a CIO, CISO, CMIO and CTO.

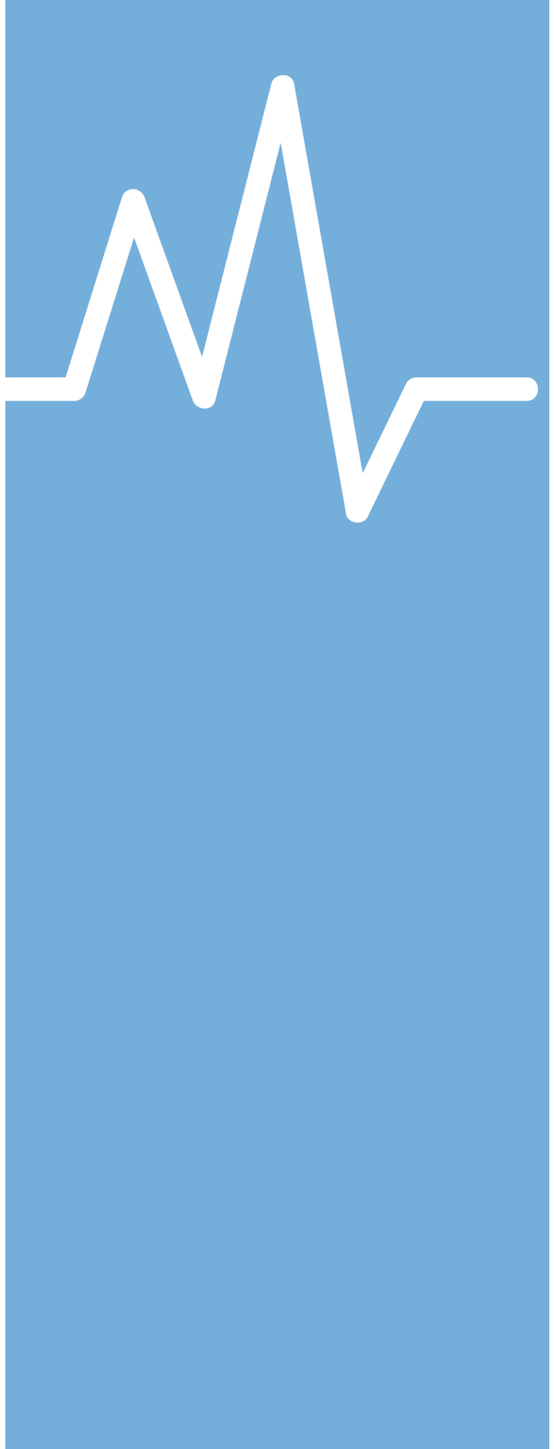


Resource Struggles

39% of organizations report their biggest challenge when it comes to implementing cyber defenses is the lack of qualified employees.

59% of healthcare organizations get at least five applications for each cybersecurity job, while 13% receive 20 or more.

- Think Managed Service Providers
- **Specialized field**
- SME varies in the different areas of cyber
- Technology is not going to fix the problem



Job Outlook: CyberSeek

National level

TOTAL CYBERSECURITY JOB OPENINGS

313,735

TOTAL EMPLOYED CYBERSECURITY WORKFORCE

715,715

SUPPLY OF CYBERSECURITY WORKERS

Very Low

CYBERSECURITY WORKFORCE SUPPLY/DEMAND RATIO

GEOGRAPHIC CONCENTRATION

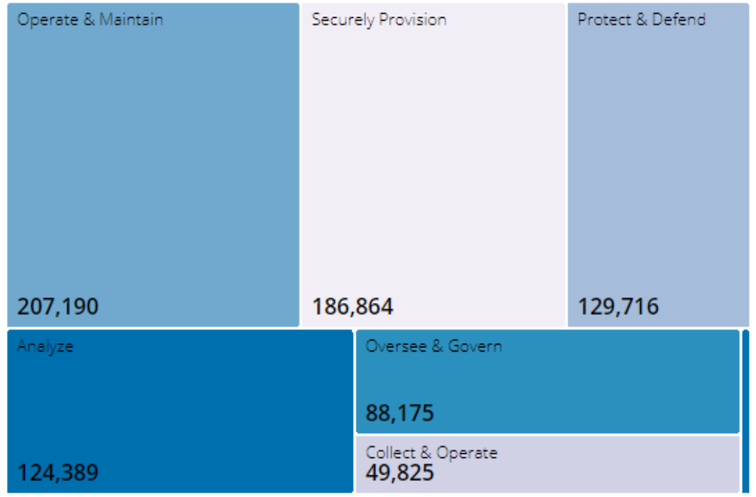
Average

LOCATION QUOTIENT

TOP CYBERSECURITY JOB TITLES

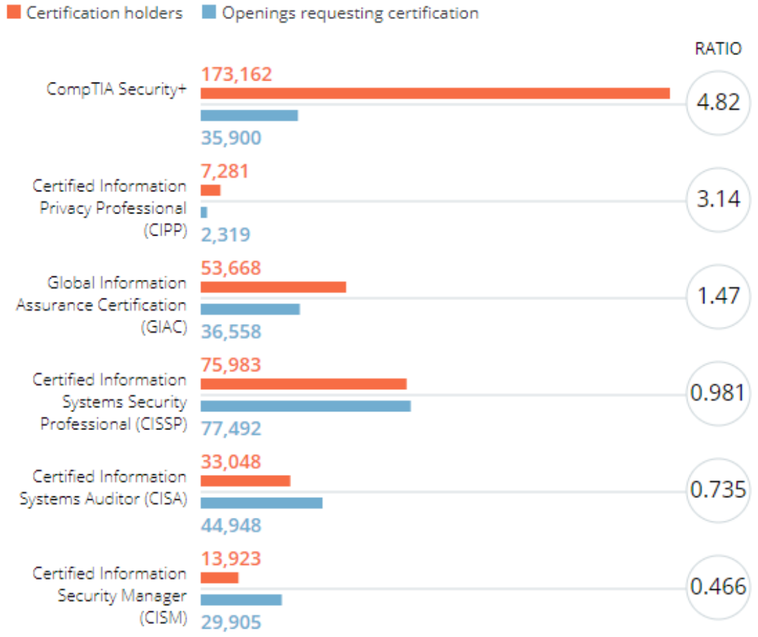
- Cyber Security Engineer
- Cyber Security Analyst
- Network Engineer / Architect
- Cyber Security Manager / Administrator
- Systems Engineer
- Software Developer / Engineer
- Systems Administrator
- Vulnerability Analyst / Penetration Tester
- Cyber Security Consultant

JOB OPENINGS BY NICE CYBERSECURITY WORKFORCE FRAMEWORK CATEGORY



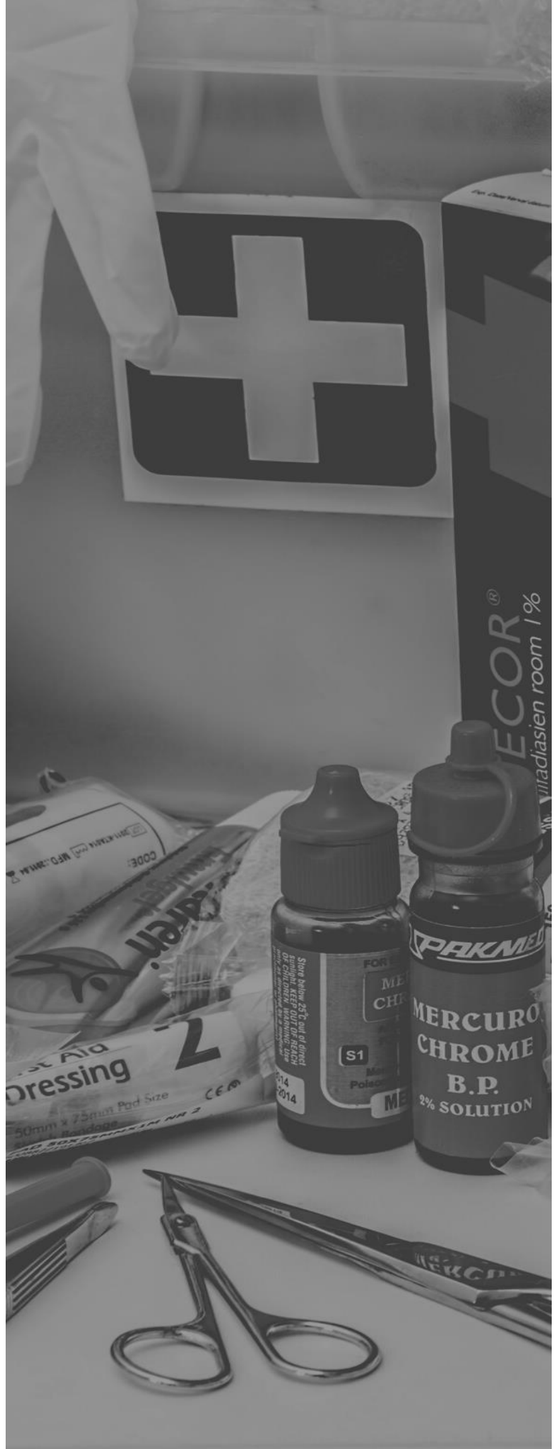
Note: The Investigate category usually has fewer openings than other categories and may not be visible in the chart. To view data for the Investigate category, please hover over the thin line in the bottom right of the visualization.

CERTIFICATION HOLDERS / OPENINGS REQUESTING CERTIFICATION



Areas of Improvement

- Access Controls
- Asset Management
- Network and Micro-segmentation
- SIEM (Threat Monitoring)
- Separation of duties



REGULATIONS FOR THOUGHT?

HIPAA

GDPR

PCI DSS

HIPAA

Security Rule

February 2003

- establishes a national set of security standards for protecting certain health information that is held or transferred in electronic form.
- Operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations must put in place to secure individuals' "electronic protected health information" (e-PHI)

Privacy Rule

December 2000

- protects all "identifiable health information" used by covered entity or its business associate; media (electronic, paper, etc.) or verbal
- Define and limit the circumstances in which an individuals health information may be used or disclosed
- Requires disclosure if requested by the individual (patient) or HHS investigation
- Is not enforced for De-identified information.

HIPAA

Security Rule

Standards

Administrative: Policy and Procedures

Technical: NIST RMF\CSF

Physical: Facility and Access Controls

PCI DSS

Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard is an information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

Assess how you store, transmit, or process cardholder data

Re-thinking Network Infrastructure

Maintaining Secure Servers AND Applications

NIST CSF crosswalk for implementation (https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework.pdf?agreement=true&time=1570899688979)

PCI Security Standards Council

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES[3]
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	• **CIS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5 • **PCI DSS v3.2.1** 6.1, 11.2, 11.3, 12.2
	ID.RA-2: Cyber threat intelligence and vulnerability information is received from information sharing forums and sources.	• **CIS CSC** 4 • **COBIT 5** BAI08.01 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC 27001:2013** A.6.1.4 • **NIST SP 800-53 Rev. 4** PM-15, PM-16, SI-5 • **PCI DSS v3.2.1** 6.1
	ID.RA-3: Threats, both internal and external, are identified and documented.	• **CIS CSC** 4 • **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 • **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 • **ISO/IEC** 27001:2013 Clause 6.1.2 • **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16 • **PCI DSS v3.2.1** 12.2

GDPR

General Data Protection Regulation

Regulation in EU law on data protection and privacy for all individual citizens of the European Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU

Google fined $57 million under the law

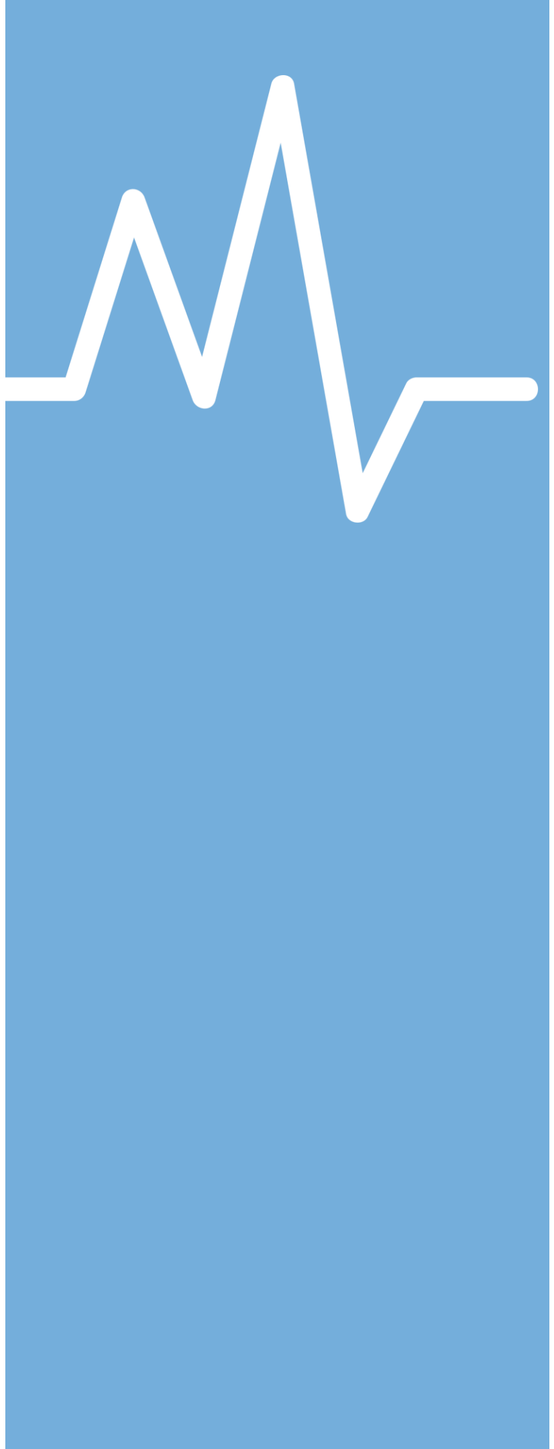
Still somewhat ambiguous for US business enforcement

International Cyber Espionage

Cyber Espionage - the act or practice of obtaining secrets and information without the permission and knowledge of the holder of the information from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage.

Cyber espionage usually focus on China, Russia, North Korea, and the United States, whether as the attacking state or the victim of attack.

These state-based threat actor teams are comprised of computer programmers, engineers, and scientists that form military and intelligence agency hacking clusters who have tremendous financial backing.



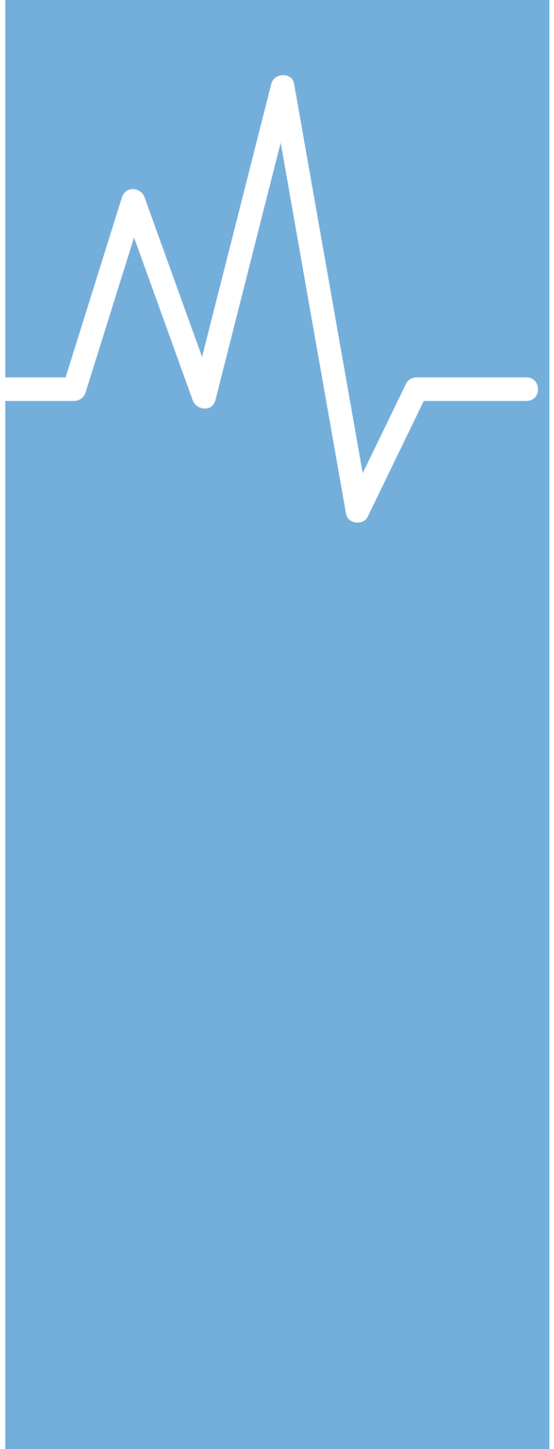
International Cyber Espionage

North Korea

- Reportedly has an army of more than 6,000 hackers that raise money to pay for the country's nuclear program.
- Sony Pictures victim in 2014, hacker group netted tens of millions of dollars
- May be responsible for the $81 million cyber heist of a Bangladeshi bank in 2016

China

- TEMP.Periscope, or Leviathan. This group has recently been escalating their attacks and targeting U.S. companies in the engineering and maritime fields
- APT10 recently attacked companies through managed service providers in multiple industries in several countries, as well as some Japanese companies, causing an unknown amount of damage through the theft of large volumes of data.



Cyber Espionage Specific to Healthcare

Actors observed targeting healthcare:
China: APT10 (Menupass) and APT41
Russia: APT28 (Tsar) and APT29 (Monkey)
Vietnam: APT32 (OceanLotus).

300 bitcoins = 2,529,735.00 USD

HEALTHCARE DATABASES (BY REGION) SOLD BY "THEDARKOVERLORD" IN 2016		
Location of Healthcare Provider	**Total Number of Records**	**Price**
Atlanta	396,459	300 bitcoins
Central/Midwest	207,572	170 bitcoins
Farmington, Missouri	47,864	60 bitcoins
Bronx, NY	34,621	25 bitcoins
United States	9,278,352	300 bitcoins
Fairview, Illinois	23,565	35 bitcoins

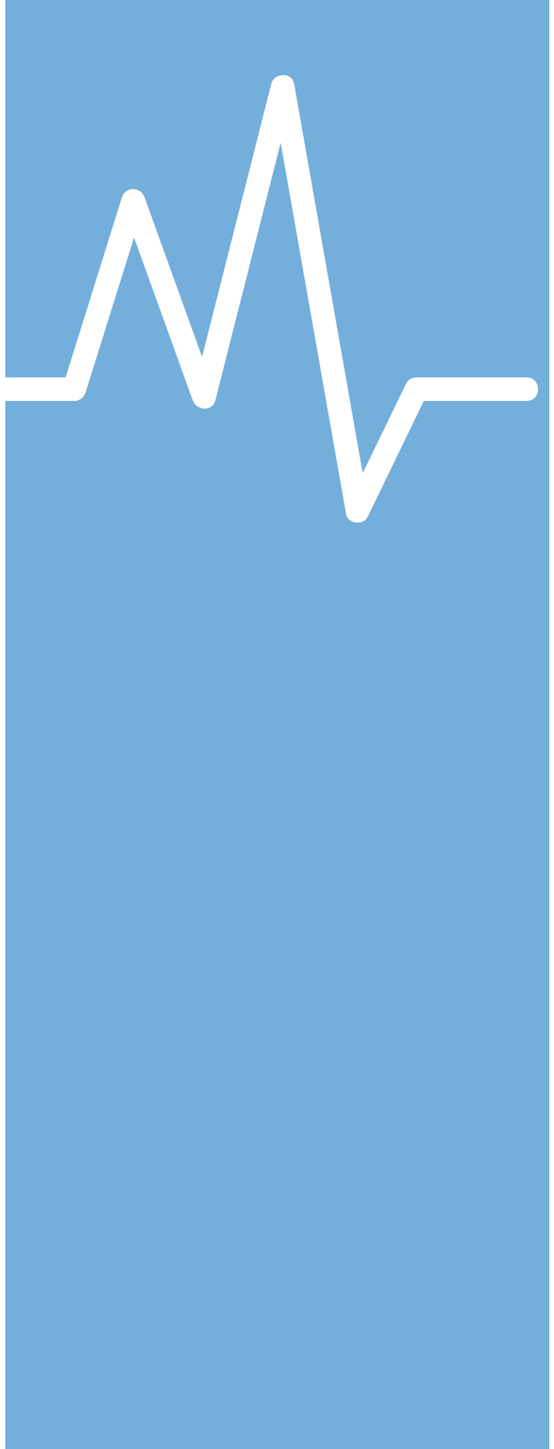
International Travel Security

China

- China International Medical Equipment Fair: 20,000-50,000 visitors
- The Health Industry Summit: 300,000 visitors
- International Conference Medical, Medicine, and Health Science: 2,000-5000 visitors

Russia

- Pharmtech and ingredients: 5,000-20,000 visitors
- Moscow Medshow: 5,000 visitors



Cyber Espionage and Travel Security

China
The Chinese government is reportedly forcing foreigners to download malware onto their phones when crossing into the country. The malware downloads people's text messages, phone logs and calendar entries, and scans the device for around 73,000 other files, according to a joint investigation

Business executives visiting luxury hotels in Asia have been infected with malware delivered over public Wi-Fi networks

Hacking devices left in hotel rooms

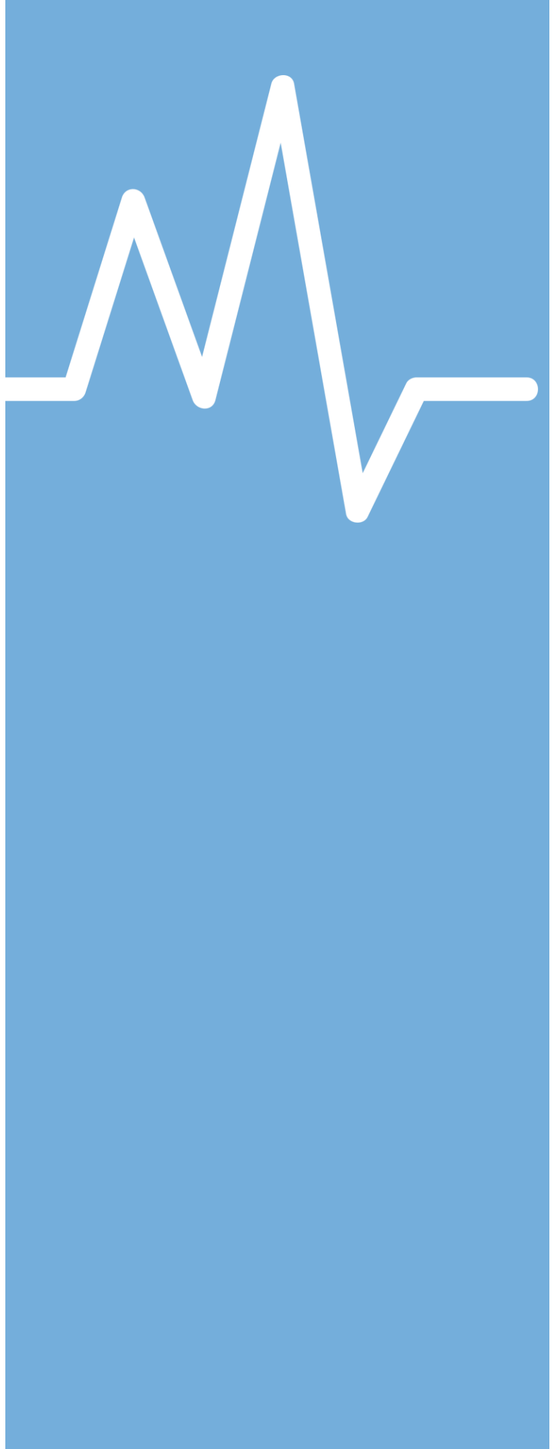
"Checking" devices in Airports

Russia
Top counterintelligence officials have advised World Cup fans travelling to Russia to leave their phones at home to avoid the prying eyes of spies and criminals.

Intelligence agencies warn that electronic devices taken to the tournament, which kicks off on Thursday, are likely to be hacked by cyber criminals or Russian agents.

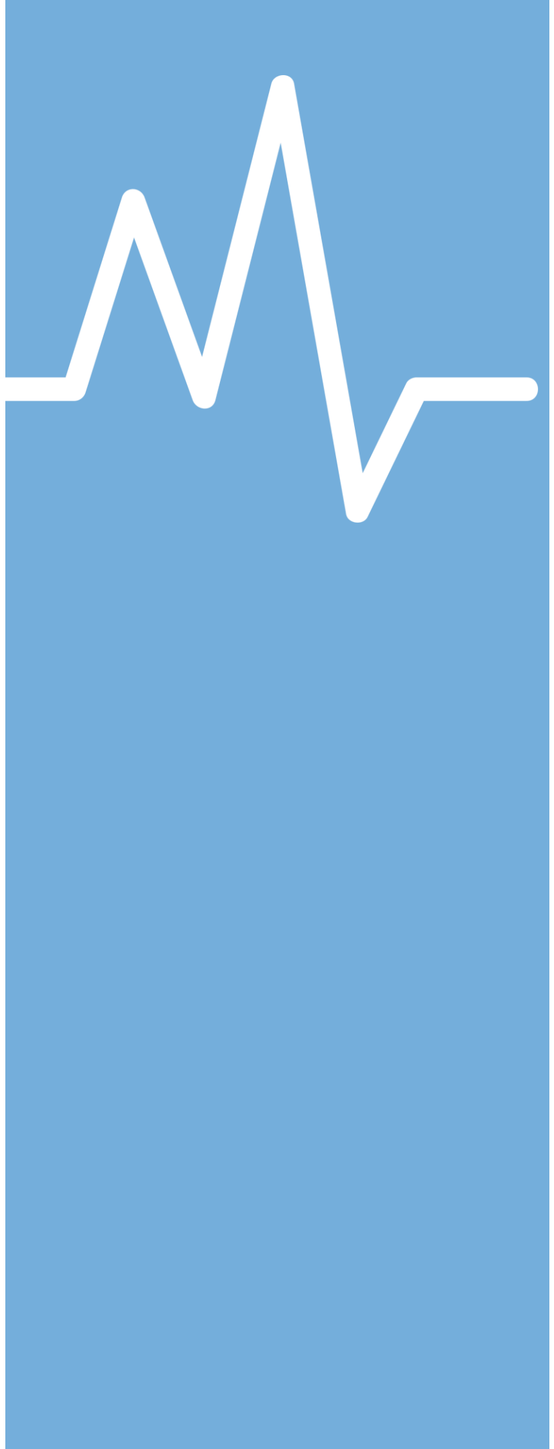
Fans who need access to a mobile should instead bring 'burner phones' that can be used at the event and then destroyed before heading home.

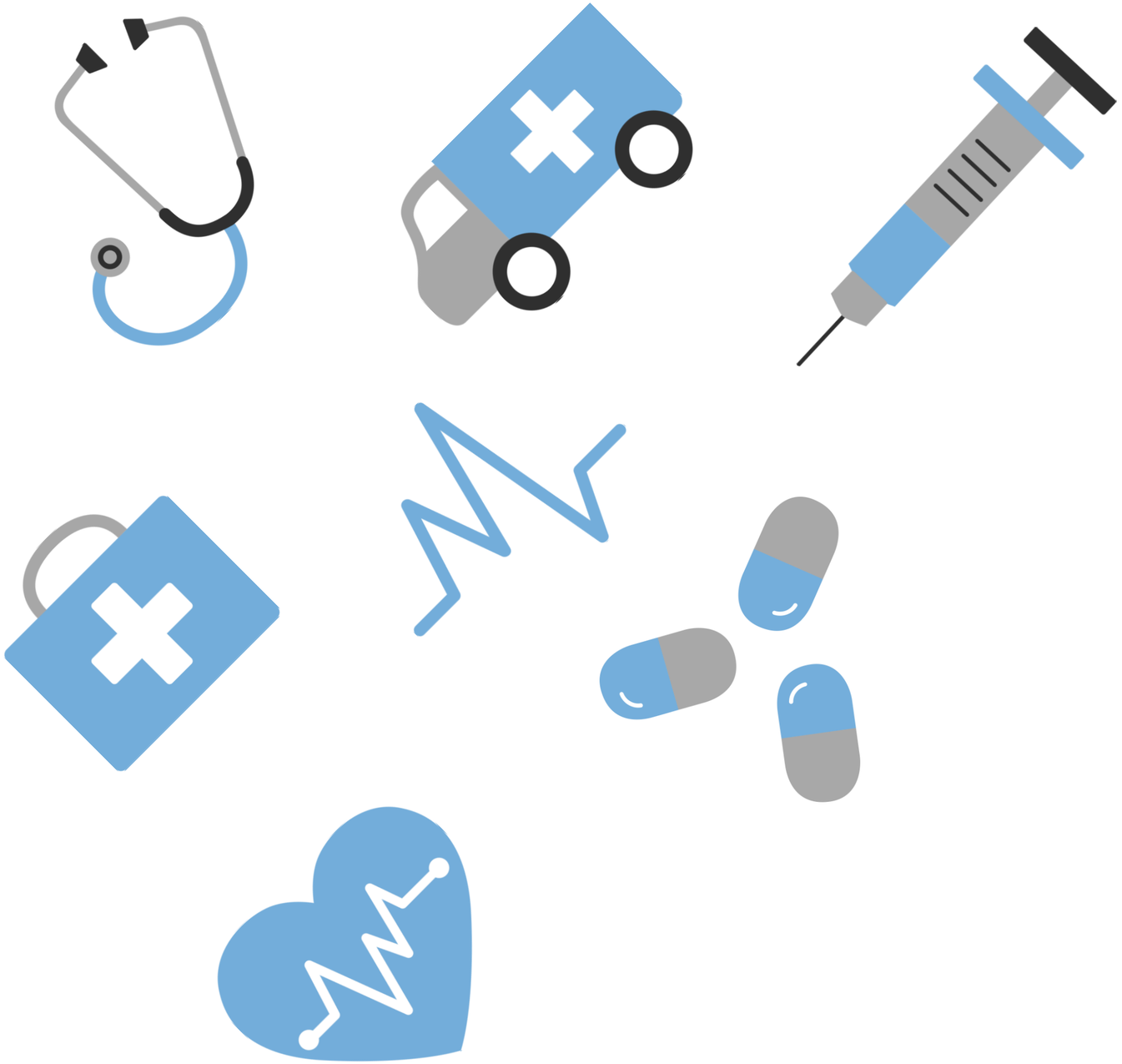
They added that fans should be wary of hotel and public Wi-Fi and keep their devices with them at all times.



International Travel Cyber Strategies

- Burner devices
- Don't use Wifi
- Don't install apps
- Don't leave devices in hotel rooms
- Develop travel Policy\Strategy for organizations





We want to hear from you!

Web

www.inherentsecurity.com

Email

trotter@inherentsecurity.com