Cybersecurity Overview
Gemini RPM Working Group

medcrypt

Axel Wirth
Chief Security Strategist

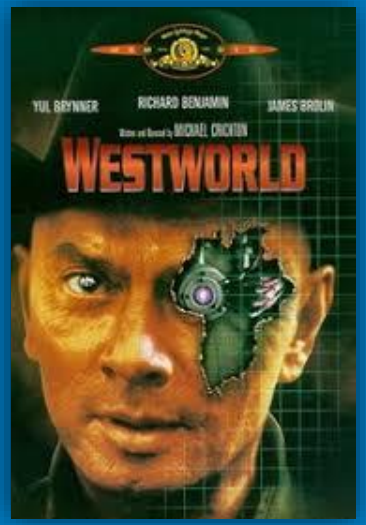
01-Sept.-2020

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices
7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

Cyber in Popular Culture

William Gibson, Neuromancer (1966) - **Cyberspace**:
"A consensual hallucination experienced daily by billions of legitimate operators, in every nation ... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data."



"There's a clear pattern here which suggests an analogy to an infectious disease process, spreading from one area to the next. …
I must confess, I find it difficult to believe in a disease of machinery."

From the Movie Westworld (1973)

What is Cybersecurity?

Security is freedom from, or resilience against, potential harm caused by others.

Examples for security categories and capabilities:

		Capabilities		
		Protection & Response	**Intelligence**	**Governance**
Categories	**National Security**	Military, Tanks	Agencies, Radar	Laws, Treaties
	Physical Security	Fences, Dogs	Cameras, Sensors	Plans, Contracts
	Cybersecurity	Antivirus, Firewall	Threat Intelligence, Event Detection	Frameworks, Standards, Policies

Of course, all are related – doors to your data center, security cameras on your network, etc.

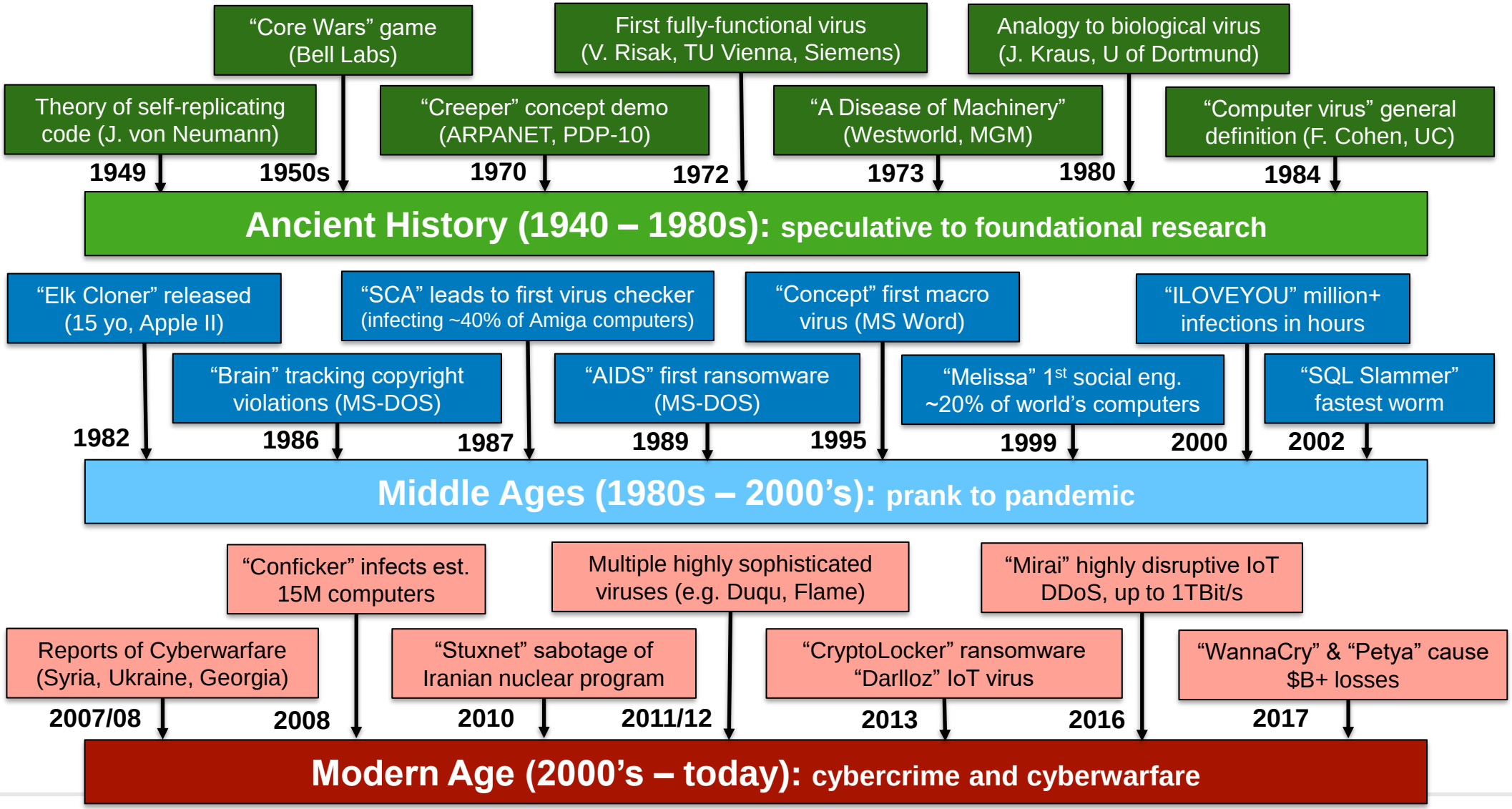
Elements of Cybersecurity

Cybersecurity spans across multiple disciplines and sciences, for example:

Engineering software, network, …	**Social Sciences** human condition and factors	**Political Sciences** laws, regulations, world politics
Physics e.g., quantum research	**Psychology** e.g., social engineering	**Economics** supply & demand, P&L, …
Mathematics cryptology, statistics, …	**Criminology** cyber crime, forensics, …	**Military Sciences** strategy and tactics of warfare

Some areas of cybersecurity are well-defined, others more ambiguous and obscure.
Consequently, teaching cybersecurity is in part facts-based, in part example-based.

Cybersecurity Timeline



The World we Live in ….. Daily Headlines

observant

Home Students Science Governance Opinion&Columns Background&Series Dossiers About us Archive
Announcements Advertisement and Paarltjes

READ HERE THE observant IN PDF

Back to list All Articles Archives Search RSS

Klik hier om onze Nederlandse website te bekijken

Cyberhack: Maastricht University pays ransom

MAASTRICHT. Maastricht University, which was hit by a cyberattack just before Christmas, paid the 'ransom' to the hackers. In doing so, the key was obtained to make systems accessible again. This was reported by well-informed sources at the UM. No official statements are being given.

It is still unclear how long it will be before all systems are working again. Interim spokesman Fons Elbersen: "For example, we won't say that the e-mail is working properly again until it is fully operational." The UM spokesman does not want to either confirm or deny the stories about any payment of ransom; the university will not make any announcements as long as the investigation into the hack and its consequences is still ongoing, also becau want to endanger the 'digital security'.

Related articles

Education programmes resume on 6 January, resits will also take place as planned
MAASTRICHT. The consequences of the cyber-attack on Maastricht University have been solved to s...

UM wants to set up 'help lines' for students and staff
MAASTRICHT. Maastricht University buildings will open on Thursday 2 January, no matter what, so...

2SPYWARE

NEWS MALWARE SOFTWARE FILES ASK US
ADWARE RANSOMWARE BROWSER HIJACKER MAC VIRUSES TROJANS

LifeLabs pays ransom to get 15M patients' records back

by Gabriel E. Hall - 2019-12-18

Add comment Ask a question 736 view

UNDERSTAND INSTANTLY

- LifeLabs releases a report about what type of customer data was put at risk after exposure
- The company claims to have paid the hacker to regain access to the lost data
- Things you can do on your own to secure personal information
- About the author
- References

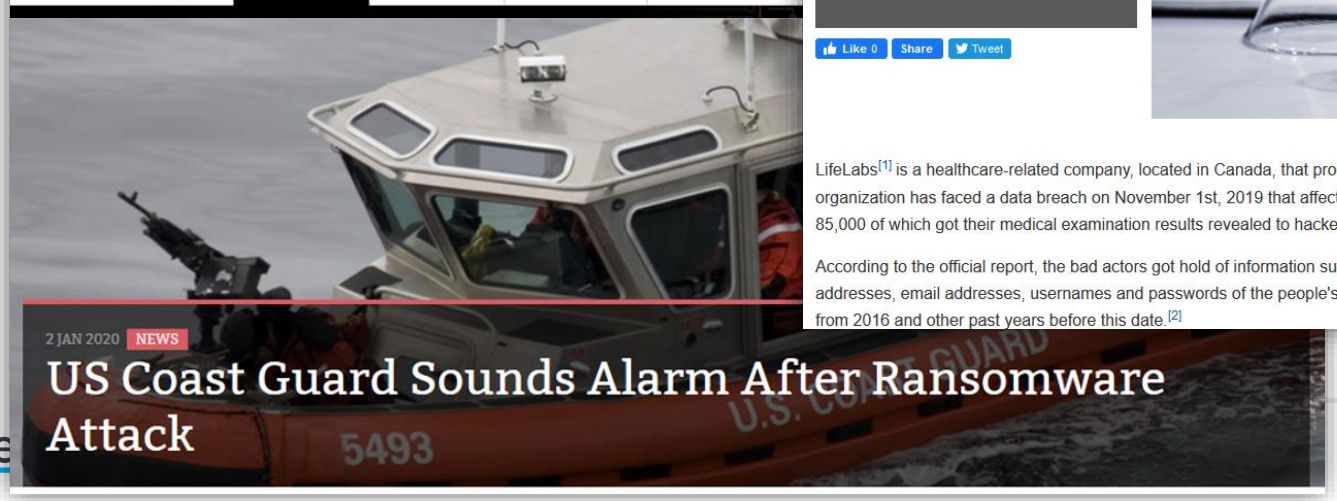
Like 0 Share Tweet

LifeLabs releases a report about what type of customer data was put at risk after exposure

LifeLabs[1] is a healthcare-related company, located in Canada, that provides laboratory diagnoses. This organization has faced a data breach on November 1st, 2019 that affected around 15 million patients' records, 85,000 of which got their medical examination results revealed to hackers also.

According to the official report, the bad actors got hold of information such as the names and surnames, residence addresses, email addresses, usernames and passwords of the people's account, and the codes of health cards from 2016 and other past years before this date.[2]

infosecurity GROUP MAGAZINE EVENTS INSIGHT



HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

Home News Features
HIPAA and Compliance Cybersecurity Cloud Mobile Patient Privacy Data Breaches

Ransomware Attacks Disrupt Patient Care at Hawaii, NJ Hospitals

Hackensack Meridian Health in New Jersey and Oahu Cancer Center in Hawaii were both hit with ransomware attacks last week, which disrupted patient care for several days.

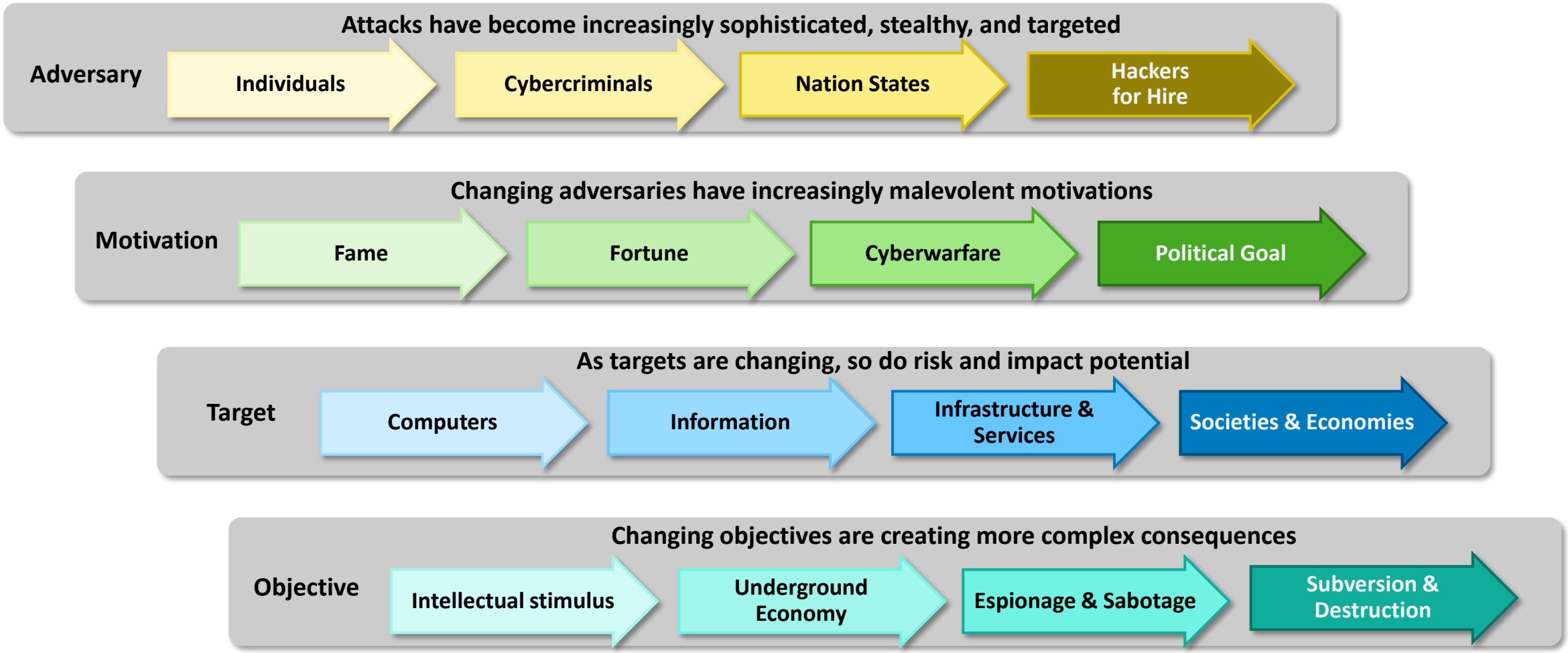
By Jessica Davis

December 16, 2019 - Two separate ransomware attacks last week took two providers offline for several days. Hackensack Meridian Health reportedly paid the ransom to bring its systems back online, while Oahu Cancer Center in Hawaii is still investigating its cyberattack.

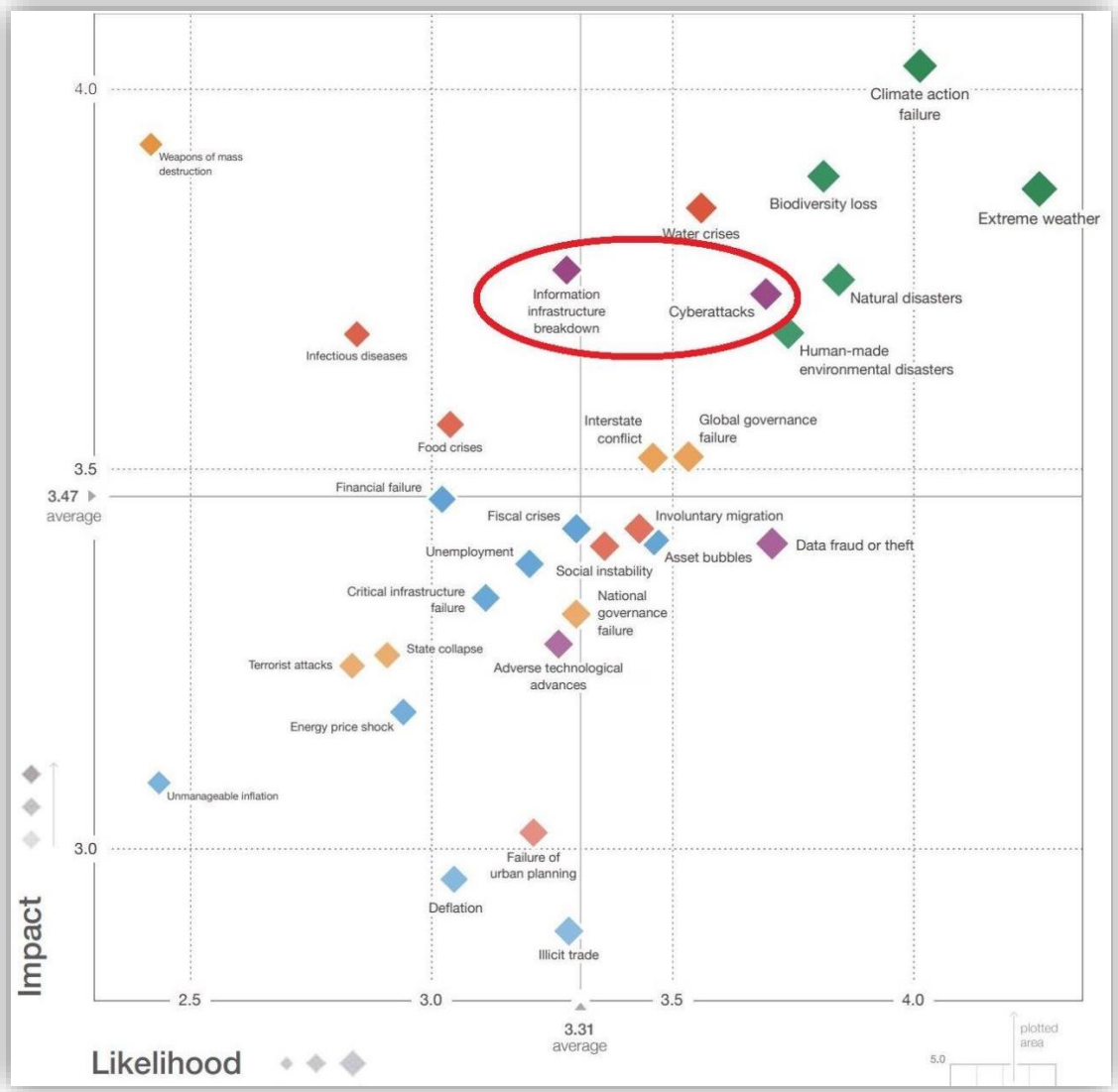
Hackers have ramped up their **disruptive** ransomware attacks on the healthcare sector in recent months, with the Office for **Civil Rights** alerting the sector to highly targeted attacks and methods to better protect their systems.

Understanding Today's Threats

Changing Adversaries and Objectives:



Global Risk Landscape 2020

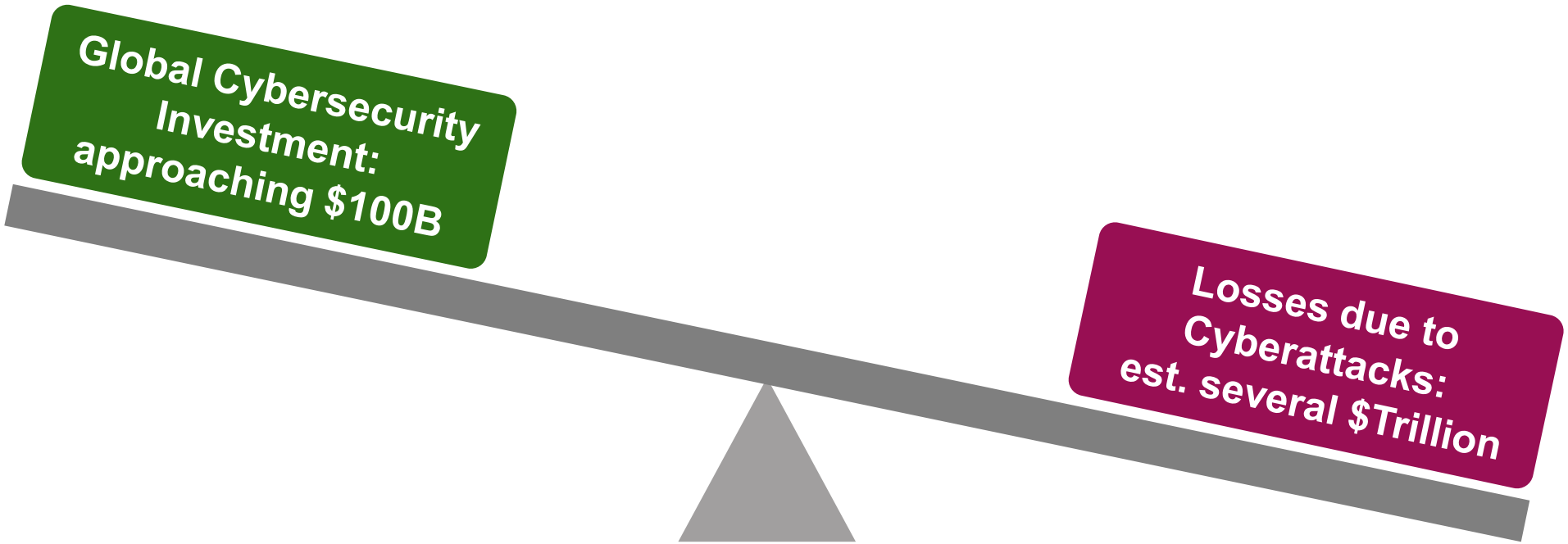


Information Infrastructure Breakdown:
Average Likelihood, above average Impact

Cyberattacks:
Above average Likelihood and Impact

World Economic Forum:
The Global Risks Report 2020
http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf

The Cybersecurity (Un)Balance Sheet



Investment (Gartner):

- 2017: $86.4 billion (up 7% over 2016)
- 2018: expected to reach $93 billion

Growing at x% (x<10)

Losses (Cybersecurity Ventures):

- ~$3 trillion today (others estimate at $1T)
- 2021: expected to reach $6 trillion

Growing by multiples

The World we Live in ….. Nation States

The "Big Four" Nation State Cyber Adversaries - Objectives:

Russia:
- Advanced Cybercrime
- Cyber Warfare (infrastructure)
- Political Goals (election interference)
- Hacking and disinformation
- Supporting the "up and coming" elsewhere

China:
- Economic growth
- Intellectual Property theft / espionage
- Blurring line between HiTech companies and government objectives
- Hackers for Hire
- Supporter and enabler of NK

North Korea:
- Developed Cyber Capabilities in response to Global Boycotts
- Supporting Government and failing Economy
- Highly advanced Cyber Criminals

Iran:
- Developed advanced cyber capabilities in response to Stuxnet
- Highly developed
- Cyber Warfare defensive and offensive capabilities

If interested: https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf

The World we Live in ….. Nation States

The "Up and Coming" Nation State Cyber Adversaries - Objectives:

Vietnam:
- Modeled after China
- Political Intelligence
- Economic Advances
- Combination of State Sponsored and Independent Actors
- Very active Underground Economy
- International and National Activities

Other Cybercrime Actors:
- Pakistan (political, cybercrime)
- Brazil (crime, mainly local and national)
- Romania (cybercrime - "Hackerville")
- Ukraine (cybercrime)

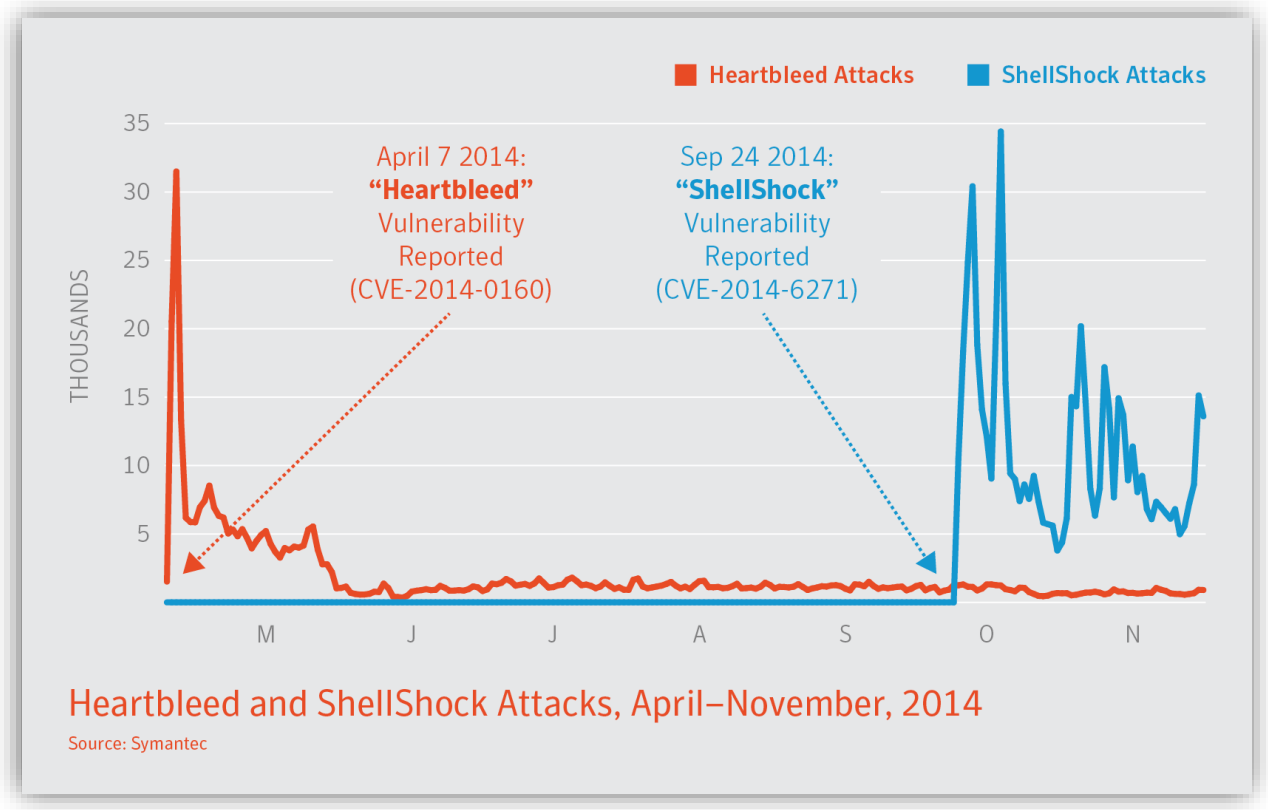
Other Middle-Eastern Countries:
- Maturing Cyber Defense
- Aggressively buying Cyber Capabilities (US, EU, Israel)
- Espionage on Business and Government
- Fueling regional tensions

Terrorists and Activists:
- Political Goals
- Cyber Guerillas and Cyber Hacktivists
- Low Threshold
- Anything is Possible
- Example: "Anonymous" attack on Boston Children's Hospital

https://www.aspeninstitute.org/programs/cybersecurity-technology-program/threat-assessment-2019/

Example: Heartbleed and Shellshock Vulnerabilities

Adversaries can pivot fast to exploit new opportunities:



Heartbleed and ShellShock Attacks, April–November, 2014

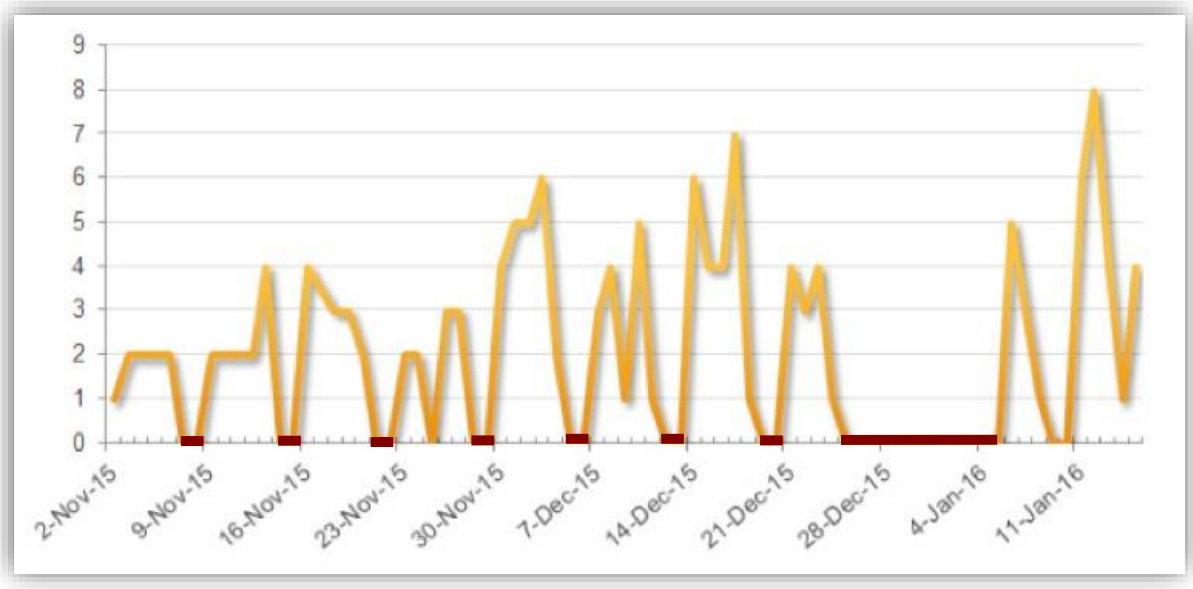
Source: Symantec

INTERNET SECURITY THREAT REPORT 2015, VOLUME 20

- Heartbleed vulnerability exploited less than **4** hours after becoming public!

Example: Professionalization of Cybercrime

Dridex Gang – Number of Known Spam Runs Per Day



"2016 Internet Security Threat Report", Symantec Corp.

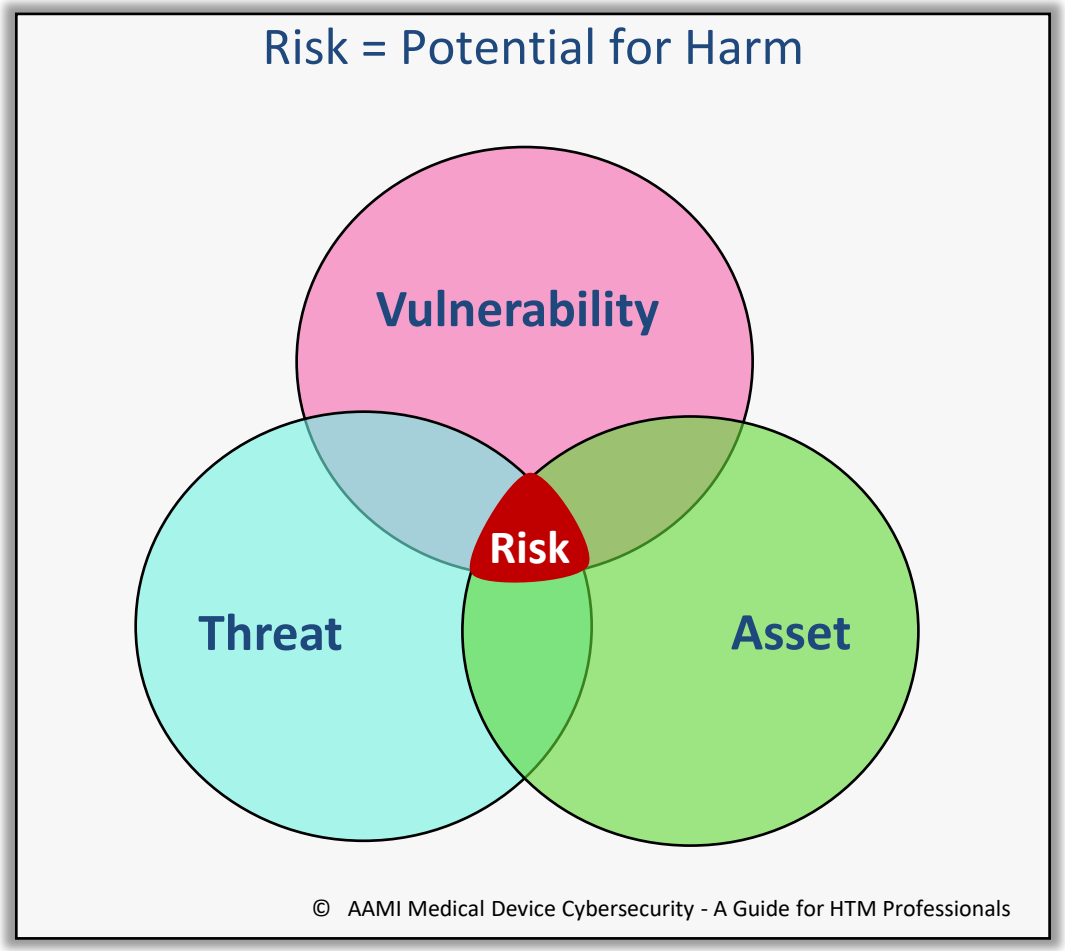
TeslaCrypt Ransomware – Technical Support Available

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices
7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

Security Terminology – Risk and Risk Components

Cyber Risk - Conceptual:



In order to have a Risk, all 3 conditions need to be fulfilled:

➔ Threat + Vulnerability + Asset = Risk
(risk is typically measured based on probability of occurrence and impact potential)

Reduction of Risk through implementation of Risk Controls:

➔ Risk – Controls = (acceptable) Residual Risk

Note: Assets can be “hard” (computers, data, money) or “soft” (reputation, trust, safety)

Agenda

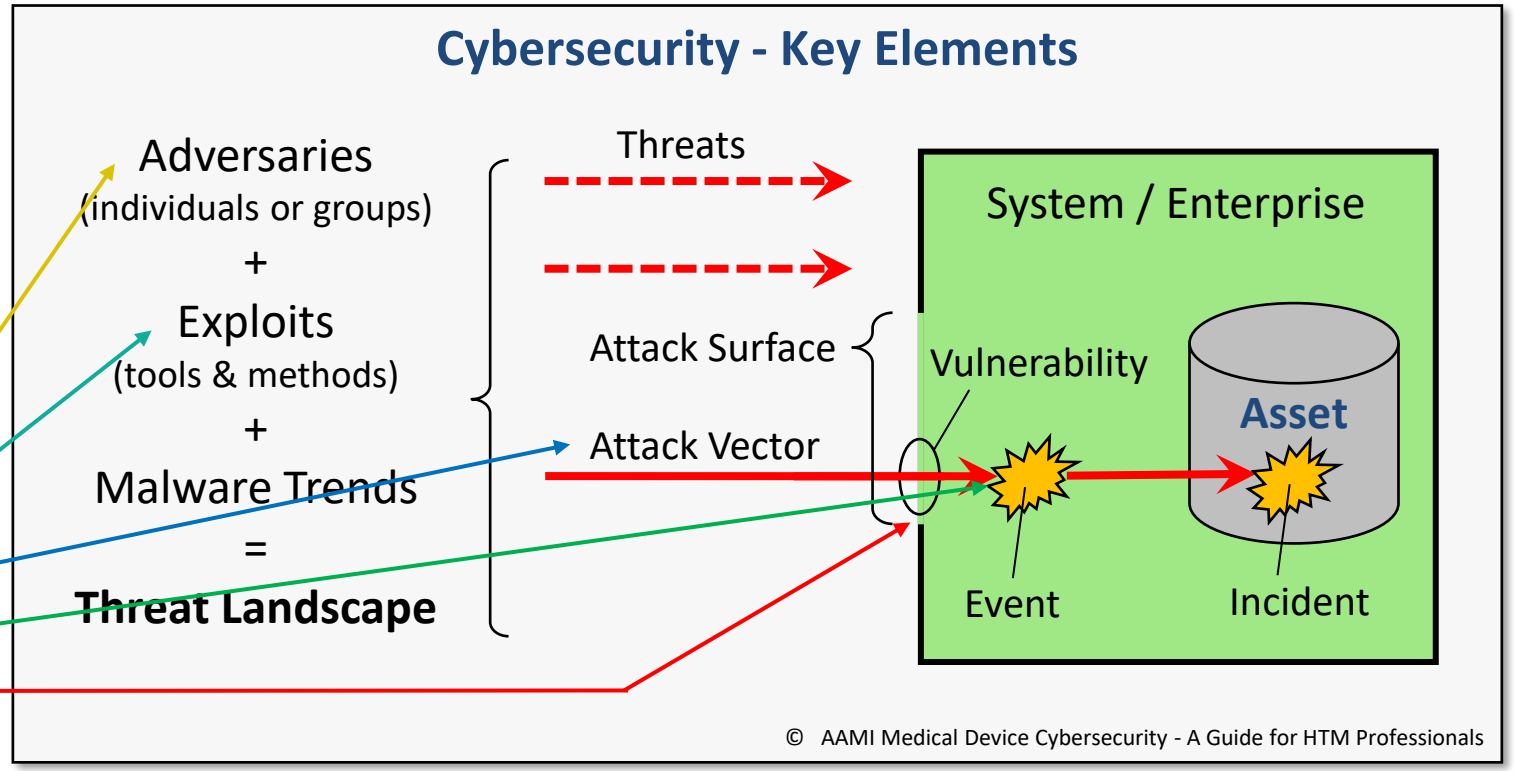
Cyber Risk – basic definitions:

- **Risk** – The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.
- **Threat** – A circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society.
- **Vulnerability** – A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard. Although most vulnerabilities are related to software, there are also hardware vulnerabilities.
- **Asset**:
  - A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.
  - Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

Security Terminology – Threat to Vulnerability

Cybersecurity – Enterprise View:

Adversary (hacking group)= Sandworm
Exploit= EternalBlue
Attack Vector= M.E. Doc
Malware= NotPetya
Vulnerability= CVE-2017-0144



Understanding the difference: An Exploit takes advantage of a vulnerability, Malware is code that performs malicious action. An adversary may use an Exploit to deliver Malware, but there are other ways to do so as well as other purposes of an Exploit.

Security Terminology – Threat to Vulnerability

Enterprise View – basic definitions:

- **Threat Landscape:** An overview of threats, together with current and emerging trends and providing a view on observed threats, threat agents and threat trends. (derived from ENISA)
- **Adversary:** An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities. May also be referred to as: threat agent, attacker.
- **Exploit**: A technique to breach the security of a network or information system in violation of security policy.
- **Attack Surface:** The set of ways in which an adversary can enter a system and potentially cause damage.
- **Attack Vector** (or: Attack Path): The steps that an adversary takes or may take to plan, prepare for, and execute an attack. *Note that an attack vector is not purely (or not always) technical and could include non-technical components as well (e.g., social engineering).*
- **Event**: An observable occurrence in an information system or network.
- **Incident:** An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Security Terminology – Threat to Vulnerability

- Requires new thinking and the combination of two approaches:
  - Traditional safety risk management
  - Traditional cyber risk management
  - Now under the umbrella of Medical Device Risk Management (see AAMI TIR 57)
- Key differences between safety and security risk management:
  - Cyber risks are, for the most, non-statistical
  - Threat (intentional) vs. Hazard (probabilistic)
  - Past experience is not a good predictor
  - Challenge: we need to operate in foresight rather than hindsight
- Yet, they are dependent on each other:
  - Security control affecting safety
  - Safety control affecting security
  - Security risks with safety impact potential

Traditional Safety Terminology	Traditional Cyber Terminology
Safety: Freedom from unacceptable risk	Security: Protection from or defense against damage, unauthorized use, or modification
Hazard	Threat
Susceptibility	Vulnerability
People, Property, Environment	Asset
Hazard (or Risk) Analysis	(Cyber) Security Risk Analysis
Misuse (reasonably foreseeable)	Exploit
Sequence of Events	Attack Vector
Hazardous Situation	Event, Incident (potential)
Harm	Incident (occurring), Consequence
Intended Use	Use Case
Probability	Exploitability
Severity	Impact

Safety vs. Cybersecurity Analogous Terminology
- These are comparable but not exact equivalent terms
- A cybersecurity safety risk analysis may require a combination

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices
7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

As Threats Evolve - Security has to, as well

Old Security

Somebody will alert you
that danger is approaching

New Security

Layered defenses, all systems, all stakeholder, test & train, automation, detection & alerting, mitigation, preparedness, response, recovery

Leave behind your "old security" mindset. Today we need a new approach … and I assume tomorrow again. Protect: Data, infrastructure, operations, and business.

In Cybersecurity, we are operating in non-linear space. Although we can analyze trends and make predictions, any event can turn the status quo on its head.

Security Technologies and Use Cases (high level)

Technology	Use Case	Trade Off	Note
Antimalware	Protect commercial and application software	Resource impact, updates, false positives	Suitable for computer-like systems; generally accepted
HIDS/HIPS (Host Intrusion Detection / Prevention System)	Protect commercial and application software via allow / deny controls	Up-front engineering effort to develop policies; limited field flexibility	Suitable for commercial OS platforms, even resource-limited systems
Cryptography	Protecting confidentiality, integrity, and authenticity	Resource requirements; protection of keys / certificates	Requires some type of supporting infrastructure to manage keys
Network segmentation	Separation of critical systems	Effort to manage and maintain; does not prevent USB attack	May not deter sophisticated hacker; does provide incident containment
Firewalls (various types)	Separation of critical systems	Does not protect from USB attack; requires maintenance	May not deter sophisticated hacker; does provide incident containment
Anomaly Detection	Network-based security, traffic inspection	Relatively new technology but maturing	Reasonable alternative to secure legacy devices

Typical Tradeoffs – Endpoint Security

Anti-Malware	HIDS / HIPS
Reactive (mainly)	Proactive
Products are constantly evolving	Products are stable and future-proof
Signature-based	Behavior and policy-based
Requires Internet (updates)	Can run stand-alone
Small but not neglectable risk of false positives	Minimal risk of false positives
Less effective on zero-days	Effective on zero-days
Requires OS integrity	Reduce patch frequency
Requires OS currency	Can effectively protect EOL OS
Large footprint	Light footprint
Customization for medical devices could reduce security capability	Requires customization but will not compromise security posture
Integrates well with enterprise security tools	Limited integration capability (depends on implementation)

Main Categories of (IT) Security Tools

Compliance and Infrastructure Management Tools

- Compliance and Vulnerability Mgmt.
- Risk Management
- Configuration Mgmt Database (CMDB)

Endpoint

- Endpoint Protection:
  - Anti-malware, SW firewall, HIDS/HIPS, Whitelisting
- "Modern" Endpoints:
  - Mobile and IoT Security
- Config. and Patch mgmt.
- Endpoint Detection & Response (EDR)

Network

- Intrusion Detection & Prevention (IDS/IPS)
- Network Access Control (NAC)
- Virtual Private Network (VPN)
- Deception (honey pots)
- Anomaly Detection

Perimeter

- Firewalls, Next Generation Firewalls
- Security Gateway
- Web Isolation
- Encrypted Traffic Inspection
- Security Analytics Recorder

Cloud

- CASB (cloud access and security broker)
- Zero Trust Platform
- Cloud-specific security solutions (server, protection , DLP, authentication, …)

Enterprise Security Tools (on premise or hosted/managed)

- Authentication
- Access control
- User Behavior Analytics (UBA)
- Cryptography-based (PKI)
- Simulation & Awareness
- Data Loss Prevention (DLP)
- Email Security
- Web Security

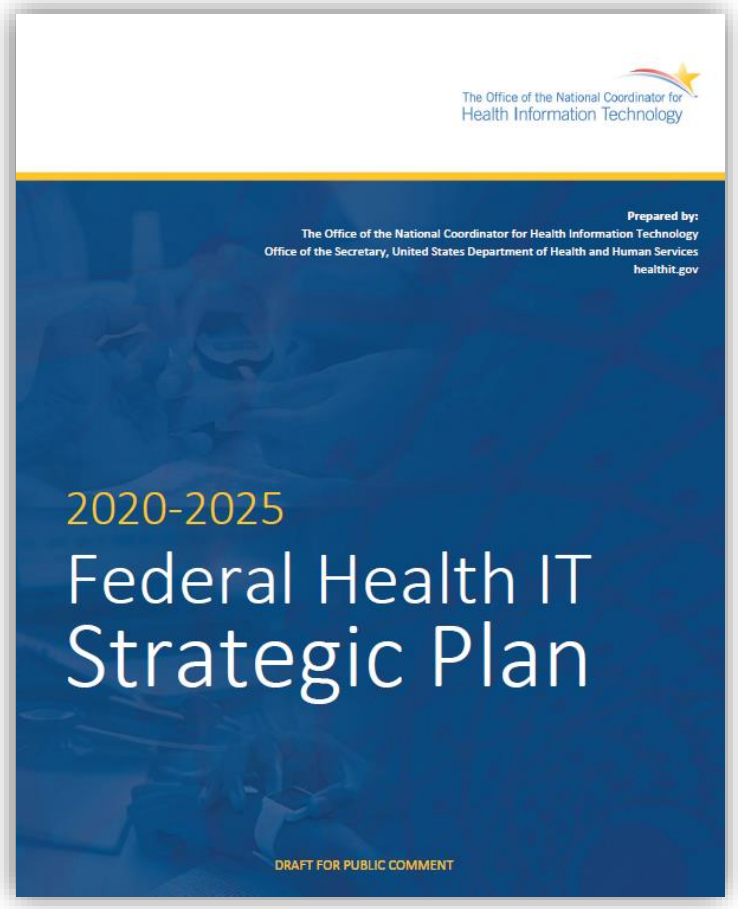
Orchestration and Response Tools (on premise or hosted/managed)

- Security Information & Event Mgmt. (SIEM)
- Security Operations Center (SOC)
- Incident Response & Remediation

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices
7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

Against all Odds – Cyberthreats Today



Despite the risk of cybersecurity attacks, breaches, and other threats, healthcare organizations still have poor understandings of cybersecurity risks and best practices.

U.S. Department of Health and Human Services Office of Civil Rights, Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance, Feb. 2019

National Health Security Strategy 2019-2022

ASPR (HHS Office of the Assistant Secretary for Preparedness and Response) Strategic Report:

U.S. National Health Security actions protect the nation's physical and psychological health, limit economic losses, and preserve confidence in government and the national will to pursue its interests when threatened by incidents that result in serious health consequences, whether natural, accidental, or deliberate.

- Identified Key Threat Areas:
  - Extreme Weather and Natural Disasters
  - Pandemic and Infectious Diseases
  - Technology and Cyber Threats
  - Chemical, Biological, Radiological, and Nuclear Threats

https://www.phe.gov/Preparedness/planning/authority/nhss/Documents/NHSS-Strategy-508.pdf

Securing Healthcare – Why is it so Hard?

- Enforcing compliance / security may conflict with care delivery (usability, ease of access, user acceptance, …)
- Complex organizations with complex decision making
- Disparate technology platforms driven by:
  - Clinical preference
  - Vendor mandate
  - Regulatory mandates slow down change
- Conservative decision making – err on the side of safety
- History and culture:
  - Compliance (HIPAA) viewed as security
  - Or even: compliance over security
- Traditionally:
  - Underinvested in cybersecurity
  - Lack of board and executive leadership on security
  - Security: hard costs, diffuse benefits

Understanding and Managing the Risks

Patient Safety

- Intentional or unintentional incidents
- Reliability, functionality, availability
- Misdiagnosis, treatment errors

Care Delivery

- Downtime due to system availability
- Impact on hospital operations
- Reduced ability to deliver care

Business & Financial

- Reputation
- Revenue / Referrals
- Law suits / fines
- Stock value

Privacy

- Confidentiality: breach of PHI, PII, credentials
- Intellectual property (clinical trials & research)
- Financial data, HR, contracts, M&A, etc.

Security

- Exploitation of a weak system – beachhead attack
- Denial of Service (DDoS) attack (origin of or impacted by)
- May be targeted or purely opportunistic

Indirect Risks

- Patient trust
- Patient treatment decisions
- Staff morale
- National Security

Healthcare's Changing Risk Priorities

From "Business Critical" over "Mission Critical" to "Life Critical"

Confidentiality

- Patient Health Data
- But also PII & PCI
- Account Information
- Billing & Payment Data
- Intellectual Property
  - Clinical Trials
  - Research
  - Designs & Formularies
- Legal & HR Documents
- Identities & Credentials

Availability

- Clinical Systems
  - Electronic Record & Specialty
  - Ancillary (PACS, Lab, Pharma)
  - ePrescription / EPCS
- Medical Devices
  - Availability of clinical services and diagnostic results
- Business Systems
  - eMail
  - Financial Systems (e.g. billing)
  - Scheduling, ERP, etc.

Integrity

- Critical Patient Data
  - Prescriptions, Medications, Dosages
  - Allergies and History
  - Diagnosis and Therapy Data
  - Alarms
- Critical Technical Data
  - Calibration
  - Safety Limits
- Functionality & reliability
  - Risk of patient harm

Patient and Staff Experience: "Trust Zone"

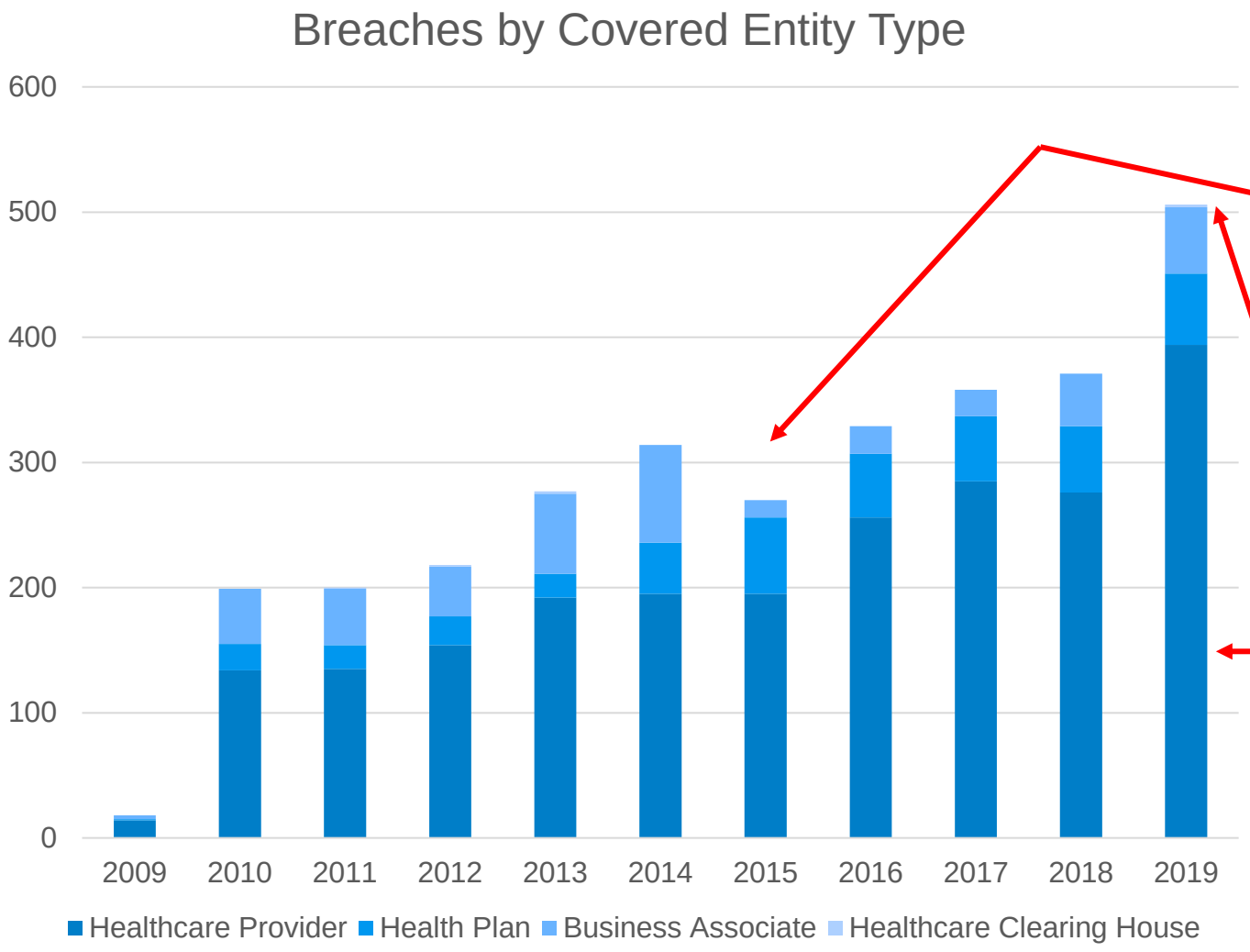
Risk of Harm: "Patient Safety Zone"

HHS Wall of Shame Analysis 2009-2019

- HITECH Act / HIPAA Breach Notification Law:
  - Since 2009, mandatory reporting of breaches over 500 records to Health and Human Services (HHS)
  - Published at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
  - Breaches <500 records are to be reported annually but are not published

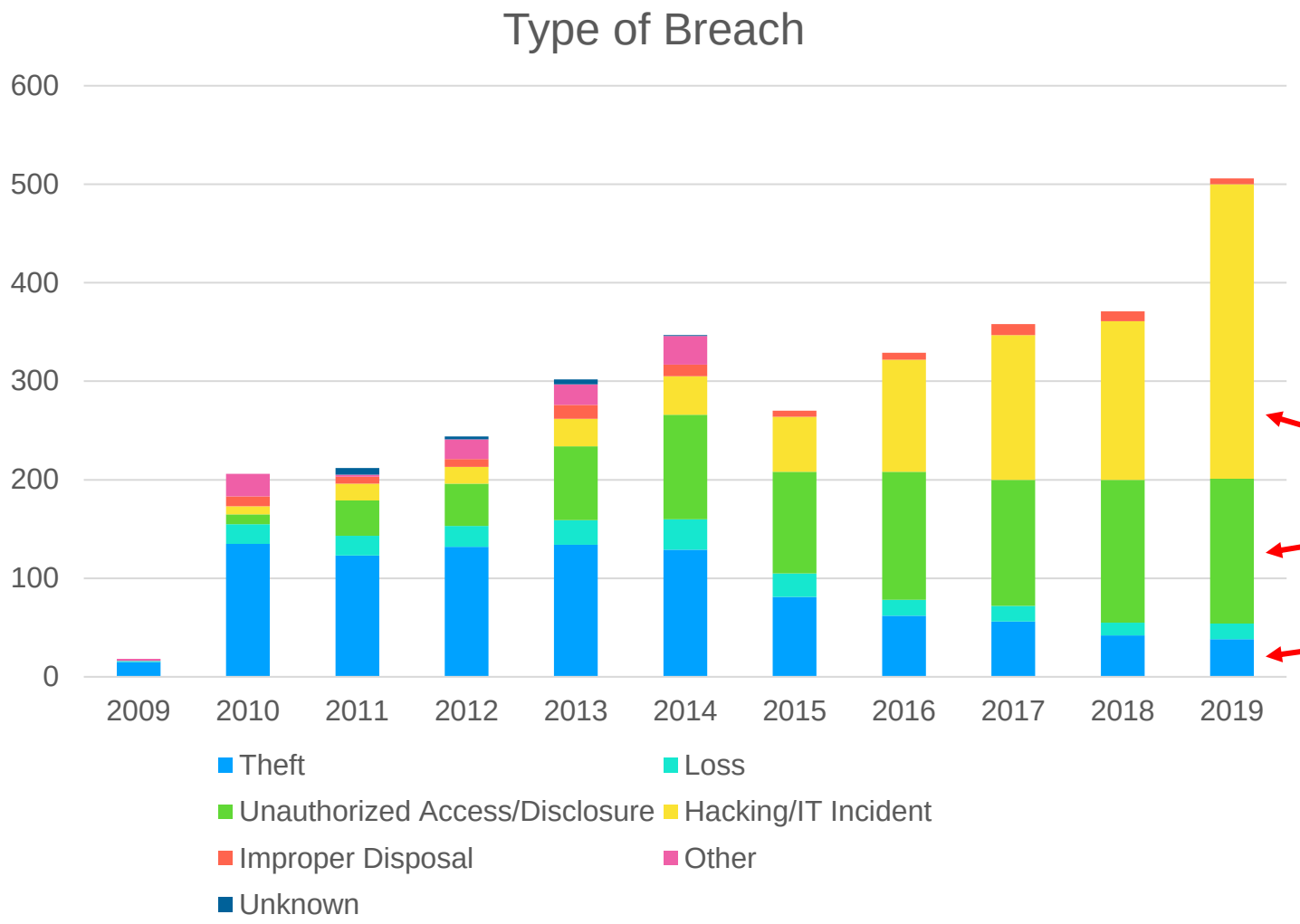
- Notes:
  - Dates are reporting dates and not incident dates, 60 day reporting window (reporting required within 60 days, but some report later)
  - Analysis based on full-year data for 2010 – 2019
  - 2009: partial reporting year (Sept-Dec)

HHS Wall of Shame Analysis 2009-2019



- 2010 → 2018:
  - 86% increase, ~10%/year
  - Only “down” year was 2015 – but highest number of breached records: 113 million
- 2018-2019:
  - 506 breaches, up from 371
  - +36% increase
  - +42% for Healthcare Providers, now accounting for 78%

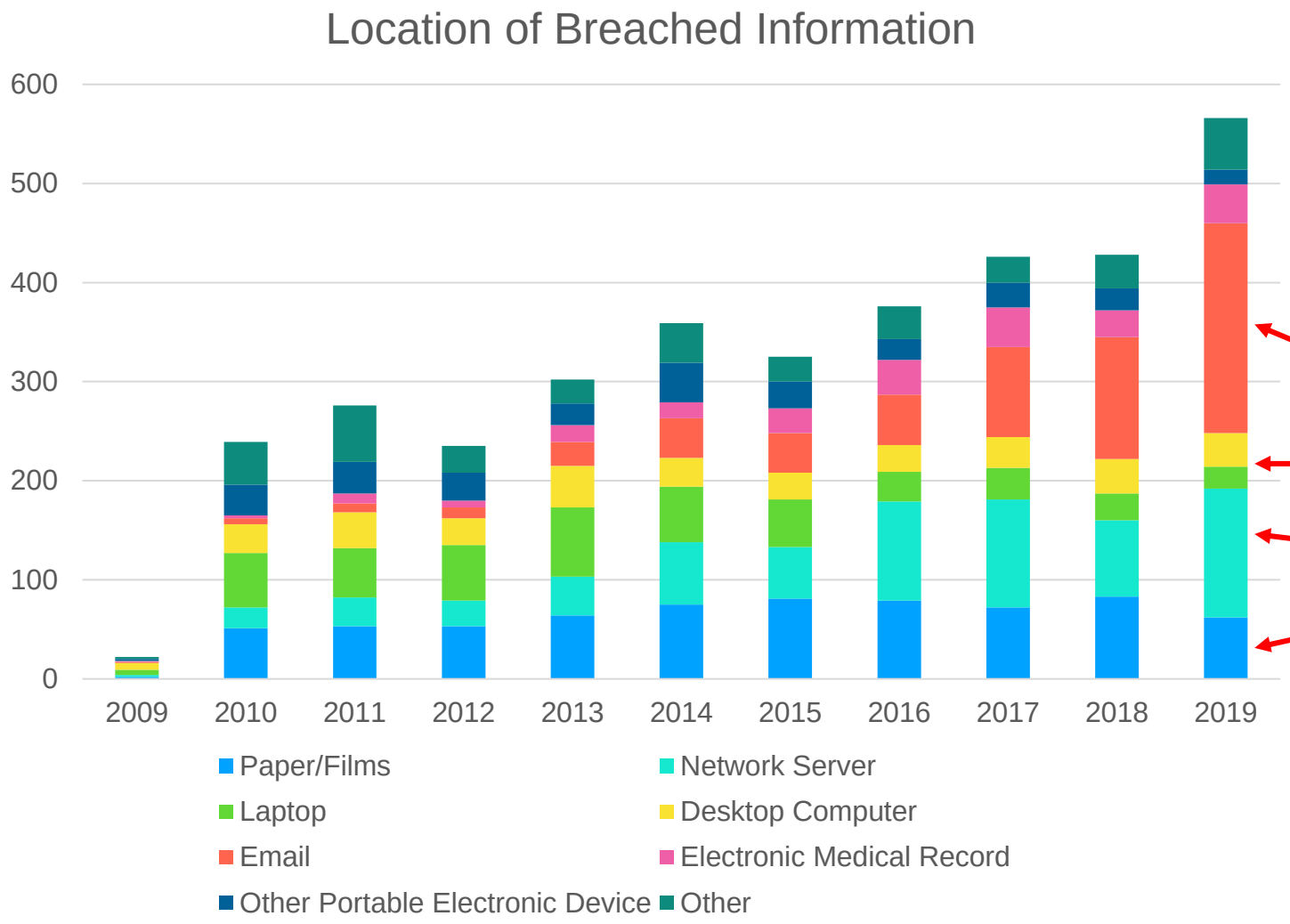
HHS Wall of Shame Analysis 2009-2019



- Total can be higher than number of breaches (multiple selections possible but less so in recent years)
- Also fewer “other” and “unknown”

- 2019 Key Conclusions:
  - 59% Hacking/IT, up from 4% (2010)
  - 29% Unauthorized Access / Disclosure, up from 5%
  - Theft down from 66% in 2010, now only 8%

HHS Wall of Shame Analysis 2009-2019



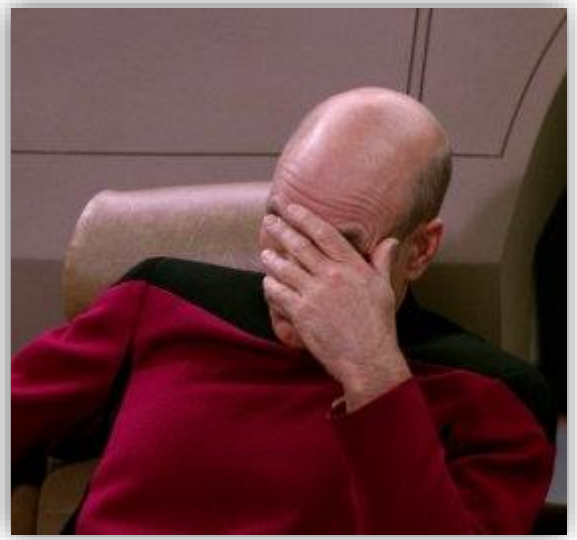
- Total can be higher than number of breaches (multiple selections possible, widely (mis)used))

- 2019 Key Conclusions:
  - 37% Email, up from 3% in 2010
  - Laptop: 4%, down from 23%
  - Desktop: 6%, down from 12%
  - 23% Network Server, up from 9%
  - Paper/Film absolute number mostly flat, but relative decrease from 20% → 10%

HHS Wall of Shame Analysis 2009-2019

Analysis of large (1m+ records) breaches

Year	1m+	
2009	0	Partial reporting year
2010	2	
2011	4	
2012	0	
2013	1	
2014	4	
2015	6	Including one 78m record breach
2016	3	
2017	0	
2018	3	
2019	5	2nd highest, ranging 1.5m to 11.5m
Total	28	



Know Thy Enemy – Many Opportunities

Attack Complexity and Impact

WIRED

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

.....

The result was more than $10 billion in total damages, according to a White House assessment confirmed to WIRED by former Homeland Security adviser Tom Bossert, who at the time of the attack was President Trump's most senior cybersecurity-focused official. Bossert and US intelligence agencies also confirmed in February that Russia's military—the prime suspect in any cyberwar attack targeting Ukraine—was responsible for launching the malicious code. (The Russian foreign ministry declined to answer repeated requests for comment.)

To get a sense of the scale of NotPetya's damage, consider the nightmarish but more typical ransomware attack that paralyzed the city government of Atlanta this past March: It cost up to $10 million, a tenth of a percent of NotPetya's price. Even WannaCry, the more notorious worm that spread a month before NotPetya in May 2017, is estimated to have cost between $4 billion and $8 billion. Nothing since has come close. "While there was no loss of life, it was the equivalent of using a nuclear bomb to achieve a small tactical victory," Bossert says. "That's a degree of recklessness we can't tolerate on the world stage."

https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Many Opportunities to Monetize

Cyber extortionists 'The Dark Overlord' offering celeb plastic surgery photos

The criminals' sophisticated PR strategy is designed to increase the pressure on victims to pay extortion demands.

10:43, UK, Friday 04 January 2019

The criminals are offering photos of cosmetic surgery. File pic.

By Alexander J Martin, technology reporter

A cyber crime group calling itself "The Dark Overlord" is offering stolen celebrities' cosmetic surgery photographs to the media to bolster an extortion campaign targeting the celebs themselves.

https://news.sky.com/story/cyber-extortionists-the-dark-overlord-offering-celeb-plastic-surgery-photos-11597618/

The Healthcare Folly – Compliance over Security

Blame it on HIPAA (Security Rule):

- Compliance is not Security (although related)
- HIPAA is just the Baseline (says HIPAA)
- It's a Regulation, not a Framework or Best Practice
- C-I-A of ePHI = limiting our risk scope (think: medical devices)
- … and it's so 2003, really

Main Requirement under HIPAA: Risk Analysis – often well-intended, but ….

- Incomplete: Assets, information, usage
- Infrequent: Annually … really?
- Serving just one regulation (HIPAA, PCI, …)
- Inconsistent: no traceability between RA's
- Lack of metrics and measurements
- Self-serving: Checklist approach, satisfy the auditor
- Manual: It's in a binder, somewhere
- Not followed through – lack of mitigation!

Changing Risk Priorities

A New Balance Between Compliance and Security

Healthcare has undergone a Paradigm Shift. Traditionally:

- HIPAA-driven priorities: Confidentiality, Integrity, Availability
- Checklist approach - satisfy the auditor

Over the past 3-5 years, Availability has become a growing concern

- Ransomware impacted information access and therefore clinical workflows
- WannaCry shut down of hospitals (UK NHS)
- Medical Device incidents have impacted care delivery

And we are starting to understand the Integrity problem

- Again, Medical Devices (hacks that could kill – but research only so far)
- Risk to critical systems and data … and Patient Trust
- Even just the perception of Loss of Integrity is a problem

Healthcare's Changing Risk Priorities

Strict Regulatory Controls need to be balanced with Nimble Security

Shifting Global Threats are leading to changing Security Priorities:

- From accidental incidents to targeted and malicious attacks
- Changing motivation: criminal attacks, political objectives
- Complex targets: devices, information, trust

	Confidentiality	Availability	Integrity
Past	Lost or stolen devices	Technical failure	Accidental alteration of data
Now	• Financially motivated • Criminal intent (ransom, blackmail) • Political attacks (nations, hacktivists)	Care delivery, e.g.: • Ransomware • Medical Devices	• Targeted attacks: intent to harm • Create doubt in data (and larger healthcare system)

"Compliance only works if your enemy is the compliance auditor"
Ted Harrington, Independent Security Evaluators

Compliance vs. Security

Traditionally, Healthcare has been a Compliance-driven Industry

Compliance
Occasional audit against well defined regulations; failure may result in fines – but you'll live

Today's Security
Any adversary, any type of conflict, unknown attack, any time, anywhere, highly skilled, no rules, any weapon – people die

Strict Compliance Controls ≠ Needs for Nimble Security

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices
7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

Agenda

1. Cybersecurity and Threat Landscape 2020
2. Cybersecurity Terminology
3. Cybersecurity Components
4. State of Security in Healthcare
5. Medical Device Security in Regulations and Standards
    a. PHD initiative and IEEE 11073 (Christoph Fischer)
    b. Regulatory context (Brian Fitzgerald)
    c. RPM NCCoE Project (Sue Wang)
6. Applying security technology to medical devices

Postponed

7. Wrap-up and Discussion
    a. Q&A
    b. Relevant topics for Gemini Technical Report

Questions?

medcrypt.com/whitepapers

axel@medcrypt.co