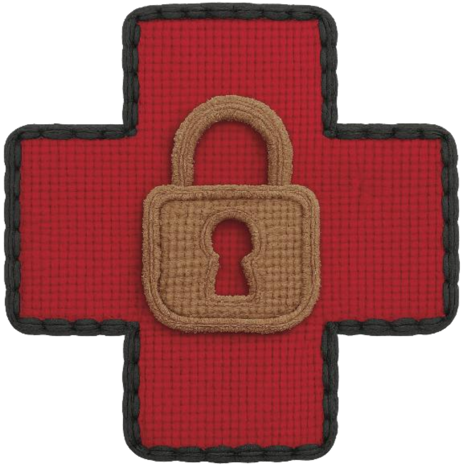
Northeastern University



Medical Device Cybersecurity – Week 3

01/20/2025 – Concepts and Terminology

Axel Wirth | Chief Security Strategist | Medcrypt

axel@medcrypt.com

Today’s Lecture

- Cybersecurity Concepts and Terminology
- Contrasting IT vs OT; safety vs security
- Relating today's threat landscape

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

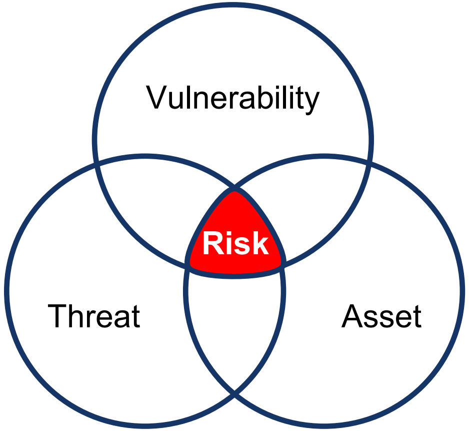
Security Terminology

Why it is Important and Sometimes gets Confused

- Medical Device Cybersecurity is rooted in part in traditional IT Security, in part in traditional Safety Risk Management.
- This accounts for a hybrid approach but also for a degree of inconsistency in terminology.
- We need to cooperate and communicate across different stakeholders with differing objectives, background, context, and technical capabilities; for example:
  - Traditional IT / IT Security
  - Safety Engineering and Privacy Professionals
  - Regulators and Standards Bodies
  - Manufacturers and Healthcare Providers
  - Clinical Staff and Clinical Engineering

PATCH

Cyber Risk – Threats / Vulnerabilities / Assets



Asset - A person, structure, facility, records, information and IT systems, resources, material, process, relationships, or reputation that has value (e.g., patient data, insurance credentials)

Threat – A circumstance or event that has the potential to exploit vulnerabilities and to adversely impact assets (e.g., ransomware)

Vulnerability – A weakness that renders an organization or asset open to exploitation (e.g., unpatched operating system)

Risk - The potential for adverse outcome, as determined by how likely it is that a particular threat will succeed in exploiting a particular vulnerability, with the associated consequences (i.e., impact on an asset, e.g. data loss or malfunction).

In order to have a <u>Cyber Risk</u>, all three conditions need to be fulfilled:

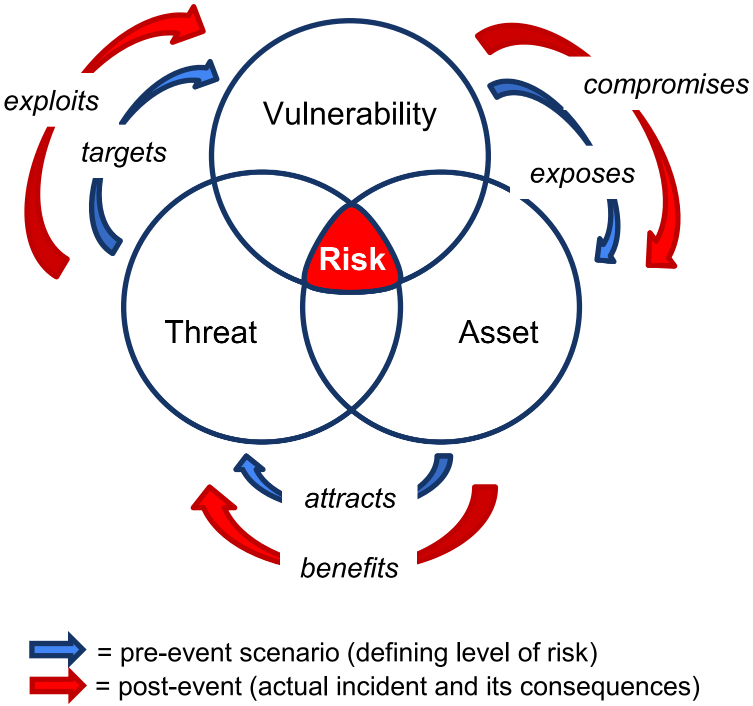
Threat & Vulnerability & Asset → Risk

Risk reduction through <u>Risk Controls</u>:

Risk – Controls → (acceptable) Residual Risk

***Note:** Assets can be tangible (computers, data, money) or intangible (reputation, trust, safety)*

Cyber Risk – Threats / Vulnerabilities / Assets



exploits
targets
Vulnerability
compromises
exposes
Risk
Threat
Asset
attracts
benefits
= pre-event scenario (defining level of risk)
= post-event (actual incident and its consequences)

Threat

- Executed by a threat actor (such as a cyber criminal group or nation state) and subject to attacker intent, choices, and capabilities
- Threats can be:
  - known (e.g., cybercriminal group, malware, etc.)
  - abstracted (e.g., Mitre ATT&CK)
  - unknown (e.g., threat modeling)

Vulnerability

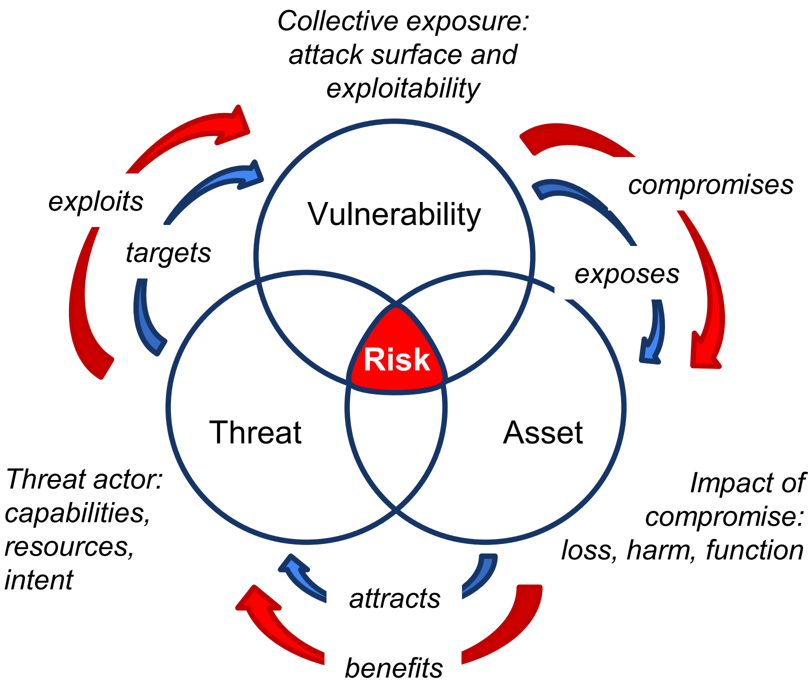
- Property resulting from design, supply chain, or implementation errors or weaknesses

Asset

- Has tangible or non-tangible value to both owner and attacker
  - but the value may not be the same (e.g., a ransomware attack may result in a $1M payment may lead to $10M of business losses)

PATCH

Cyber Risk – Threats / Vulnerabilities / Assets



Collective exposure: attack surface and exploitability
exploits
targets
Vulnerability
compromises
exposes
Risk
Threat
Asset
Threat actor: capabilities, resources, intent
Impact of compromise: loss, harm, function
attracts
benefits

Estimating Risk:

- Requires an abstract model based on Likelihood of Occurrence and Impact
- Use quantitative (e.g., L, M, H) or semi-qualitative (e.g., 1 - 4 scale) measures
- In cybersecurity Likelihood cannot be calculated using statistical methods, it can be estimated

Different Approaches:

- Vulnerability-centric view → “Exploitability”, i.e., an estimate of the ease of exploitation.
- Risk-centric view → “Security Risk” is assessed by combining the likelihood that a threat will successfully exploit a vulnerability and result in an impact on an asset (severity of that impact).
- However, nuances apply, e.g., :
  - Intentional vs. unintentional attacks
  - Premarket – consider exploitability and abstract threats
  - Postmarket – consider risk and criticality as e.g., evident by observed incidents

Security Terminology – Risk Control Concepts

- Risk Control – *As outcome of your risk management process (discussed later in more detail), risk controls reduce the probability or severity of a potential incident to an acceptable level through:*
  - *Mitigation: preventive measures – reducing the “probability” and/or “severity”, e.g., antimalware software*
  - *Contingency: reducing the consequences – i.e., the “severity”, e.g., backup*
  - *Transfer: of risk to another party, e.g., through insurance, labeling, etc.*
  - *Acceptance: if probability and severity are low enough that the risk is sufficiently reduced*
- Risk Mitigation – The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or lessen its consequences. Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives.

Example for
Risk Mitigation

Example for
Risk Transfer

Cybersecurity Risk Analysis

Risk-Management through estimation, prioritization, and treatment.
Risk-Estimation:

- Historical data may not be available and is of limited value
- Hence, we use the forward-looking concept of “exploitability”

Example for semi-quantitative Risk-Estimation:

- Estimate Likelihood and Impact
- Likelihood not used in the mathematical sense, it is used as a measure of “ease of exploitation”
- Risk-Estimate L x I = R
- Prioritize based on score
- Complex models may use multiple parameters (e.g., CVSS)

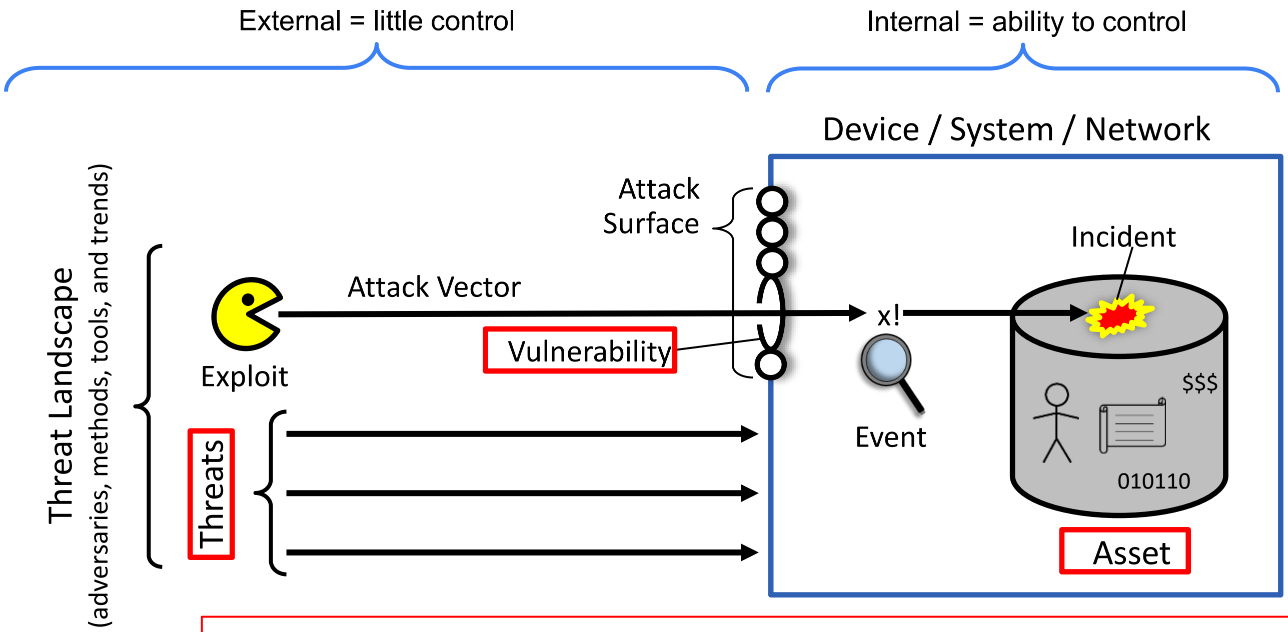
Notes:

- A 4x4 matrix only an example
- Other methods exist
- Don’t overdesign your system – it’s an estimate

Likelihood (of harm)

Impact (of harm)	Improbable 1	Remote 2	Occasional 3	Probable 4
Catastrophic 4	4	8	12	16
Critical 3	3	6	9	12
Marginal 2	2	4	6	8
Negligible 1	1	2	3	4

Summarizing: Cybersecurity Terminology


External = little control
Internal = ability to control
Device / System / Network
Attack Surface
Incident
Attack Vector
x!
Threat Landscape
(adversaries, methods, tools, and trends)
Vulnerability
Exploit
$$$
Event
Threats
010110
Asset

Estimated Risk = Likelihood of Occurrence x Severity of Impact

But context is important to select the right approach and model

- Likelihood – may be expressed as Exploitability (e.g., for vulnerability scoring)
- Severity – may be expressed as Level of Harm (e.g., for safety risks)

Summarizing: Cybersecurity Terminology

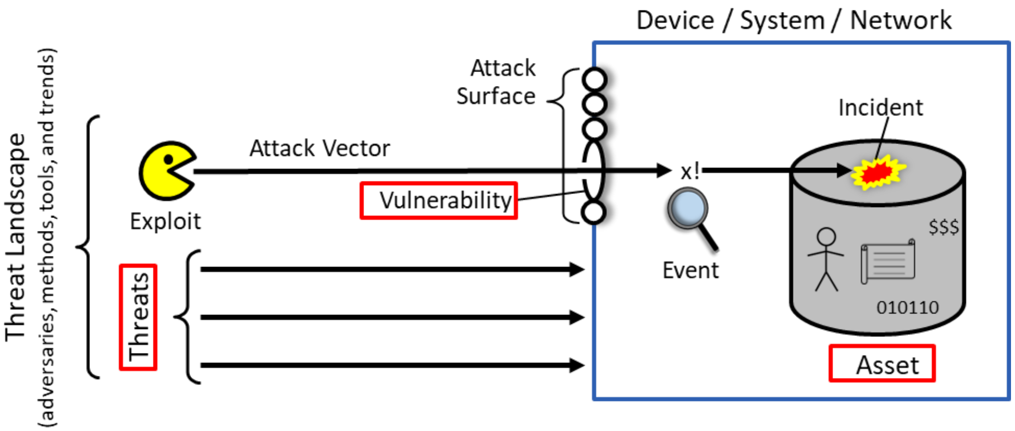
The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

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

Example:

Threat Actor = Sandworm hacker group
Exploit = EternalBlue
Malware = NotPetya
Attack Vector = M.E. Doc software
Vulnerability = CVE-2017-0144



Note: often confused or “used as equivalent” terms:

- Event ≠ Incident (but an Event may lead to an Incident)
- Exploit ≠ Malware (but an Exploit may utilize Malware(s))

Security Terminology - 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.

Note: the distinction between Event and Incident is subtle and many (incorrectly) use the terms interchangeably.

Security Terminology – Other Terms

- ***Breach:*** *A somewhat vaguely defined term:*
  - *Typically referring to a security incident that results in unauthorized access to or exfiltration of data, i.e., it specifically refers to a data breach. This is the more common use of this term in healthcare, e.g., HIPAA Breach Notification Law.*
  - *In the more general context, it may be more used to describe a security breach, i.e., in general terms an incident that results in unauthorized access of data, applications, services, networks and/or devices.*
- **Consequence:** The effect of an event, incident, or occurrence.
- **Compromise:** Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. *Note that a compromise may be the result of an intentional (targeted) or unintentional action.*
- **Indicator of Compromise (IoC):** An occurrence or sign that an incident may have occurred or may be in progress.
- **Malware:** *short for malicious software.*

Any other computer or security term you may encounter: https://csrc.nist.gov/Glossary (10,000+ and counting)

Today’s Lecture

- Cybersecurity Concepts and Terminology
- Contrasting IT vs OT; safety vs security
- Relating today's threat landscape

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

Safety Risk vs IT Risk vs Product Cyber Risk

“All models are wrong; some models are useful”

Safety Risk Management

- Based on past experiences (e.g., returned goods, complaints, failures, testing, …)
- Hazards are generally known (e.g., environmental factors like temperature)
- Malicious intent should be considered but is the exception - “reasonably foreseeable misuse”
- Using statistical methods to calculate probability of occurrence
- Reduce future risk through design improvements, etc.

IT Cybersecurity Risk Management

- Using present knowledge of cyber threats and vulnerabilities to minimize risk exposure
- Updated on a regular basis to identify new risks (assets, vulnerabilities, and threats)
- Mitigate reactively (e.g., patching)
- Reduce future risk exposure through regular updates and replacement

Product Cybersecurity Risk Management

- Forward-looking – a reactive approach to security, although not totally avoidable, is less desirable
- Known and unknown (future) threats
- Past experience and statistical analysis of limited value
- Estimating risk through modeling
- Reducing risk through management of vulnerabilities and exposure of assets

So Many Concepts – So Little Time

Safety vs Cybersecurity Risk Management

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

Safety vs. Cybersecurity, Analogous Terminology

Notes:

- These are comparable but not exact equivalent terms.
- A cybersecurity safety risk analysis may require considering a combination.
- One of the fundamental differences is that a Threat is typically intentional, a Hazard (in most cases) coincidental.

Cyber-Physical Cybersecurity – Contrasting IT and OT

Information Technology (IT) vs. Operational Technology (OT)

"A Tale of Two Cities"	Traditional IT	Operational Technology (OT)
Example:	Workstations, Servers, Mobiles	Medical Devices, HVAC, Fridges
Priorities:	C – I – A: Mission Critical	A – I – C: Safety Critical
Regulation:	Some; risk of fines	Highly regulated; risks of fines & jail
Technology Life:	3 to 5 years	5 to 10+ years
Security Posture:	Homogeneous, mature	Complex, immature, weakest link
Change Management:	Regular, automated	Slow, manual, many dependencies
Window of Vulnerability:	Days to weeks	Months to years
Downtime:	Acceptable (planned, unplanned)	Difficult, 24 x 7 x 365 operation
Risk (impact):	Data & operations	Safety, operations, destruction
Risk (duration):	Short to medium	Medium to long
Recovery:	Restore system & data	Restore; rebuild physical systems

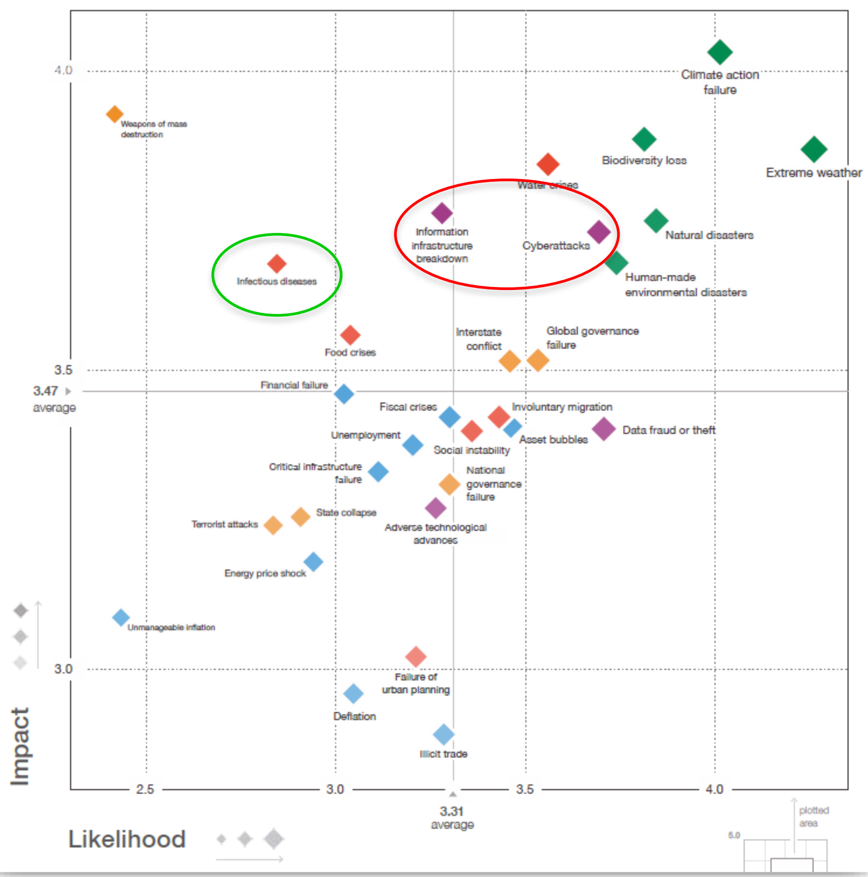
Today’s Lecture

- Cybersecurity Concepts and Terminology
- Contrasting IT vs OT; safety vs security
- Relating today's threat landscape

Note – I may pull images off the WWW to give examples and support my explanation.
None of this should be considered endorsement of a specific product or vendor.

PATCH

Global Risk Landscape 2020



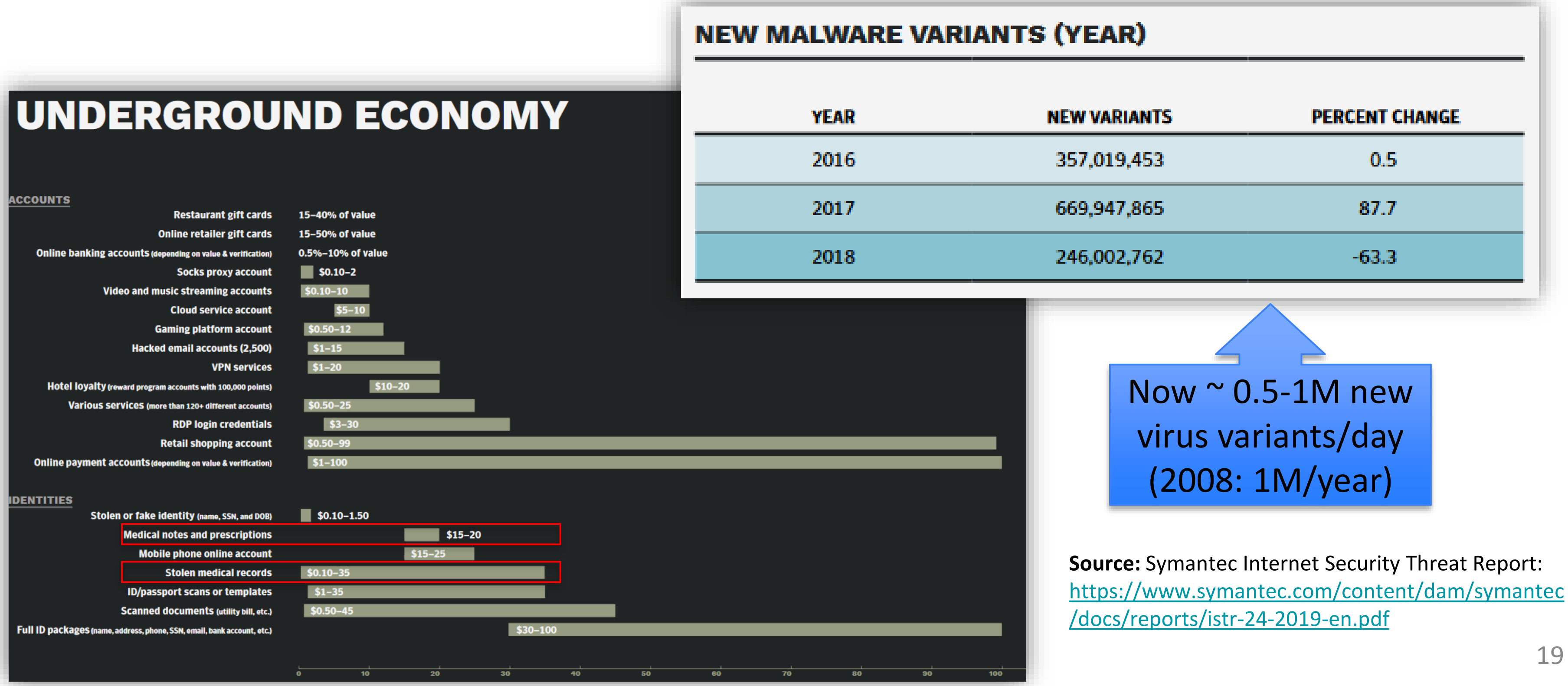
Another important lesson we learned – just because something is classified as low likelihood does not mean it will not happen

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

Understanding Today’s Threat Landscape - Examples



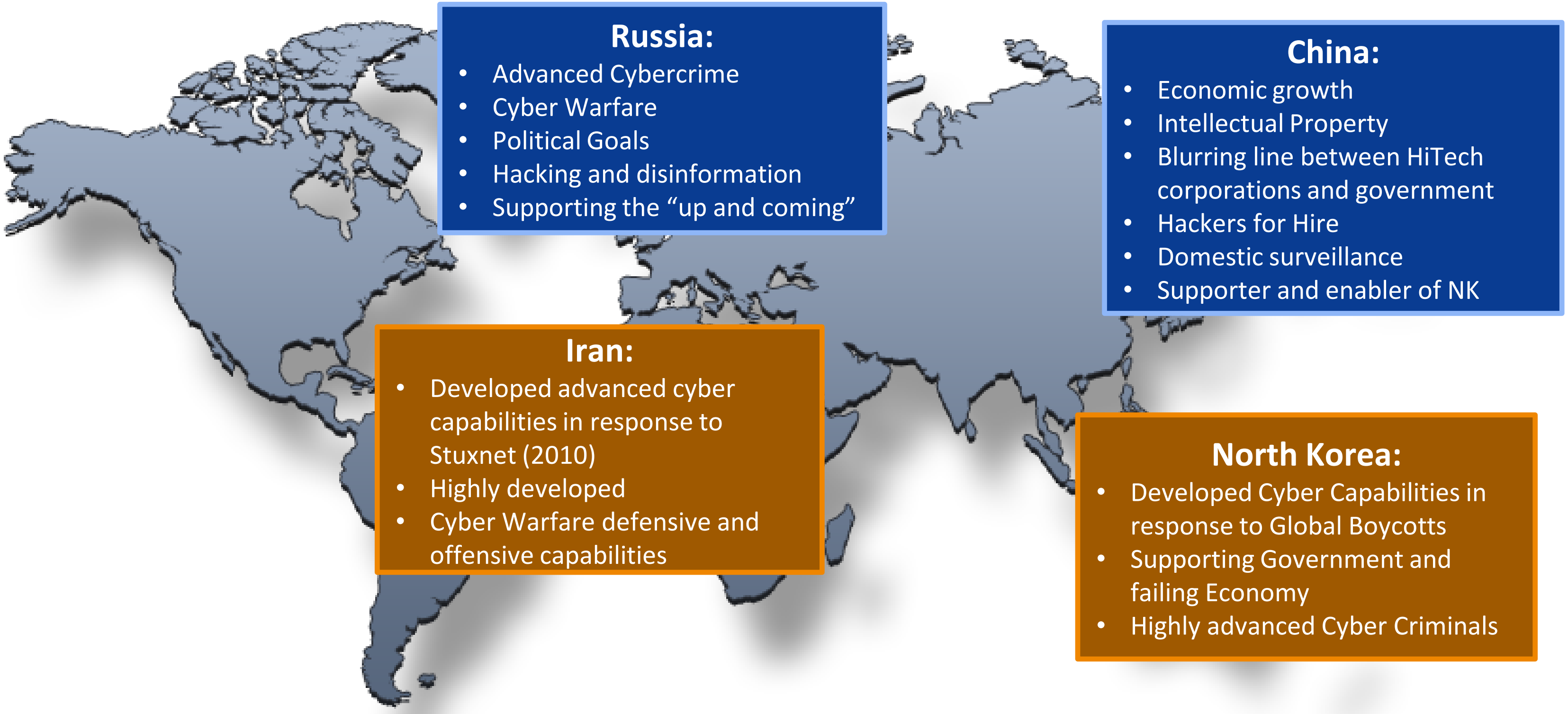
NEW MALWARE VARIANTS (YEAR)

YEAR	NEW VARIANTS	PERCENT CHANGE
2016	357,019,453	0.5
2017	669,947,865	87.7
2018	246,002,762	-63.3

Now ~ 0.5-1M new virus variants/day (2008: 1M/year)

Source: Symantec Internet Security Threat Report: https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf

The “Big Four” Nation State Cyber Adversaries



Russia:

- Advanced Cybercrime
- Cyber Warfare
- Political Goals
- Hacking and disinformation
- Supporting the “up and coming”

China:

- Economic growth
- Intellectual Property
- Blurring line between HiTech corporations and government
- Hackers for Hire
- Domestic surveillance
- Supporter and enabler of NK

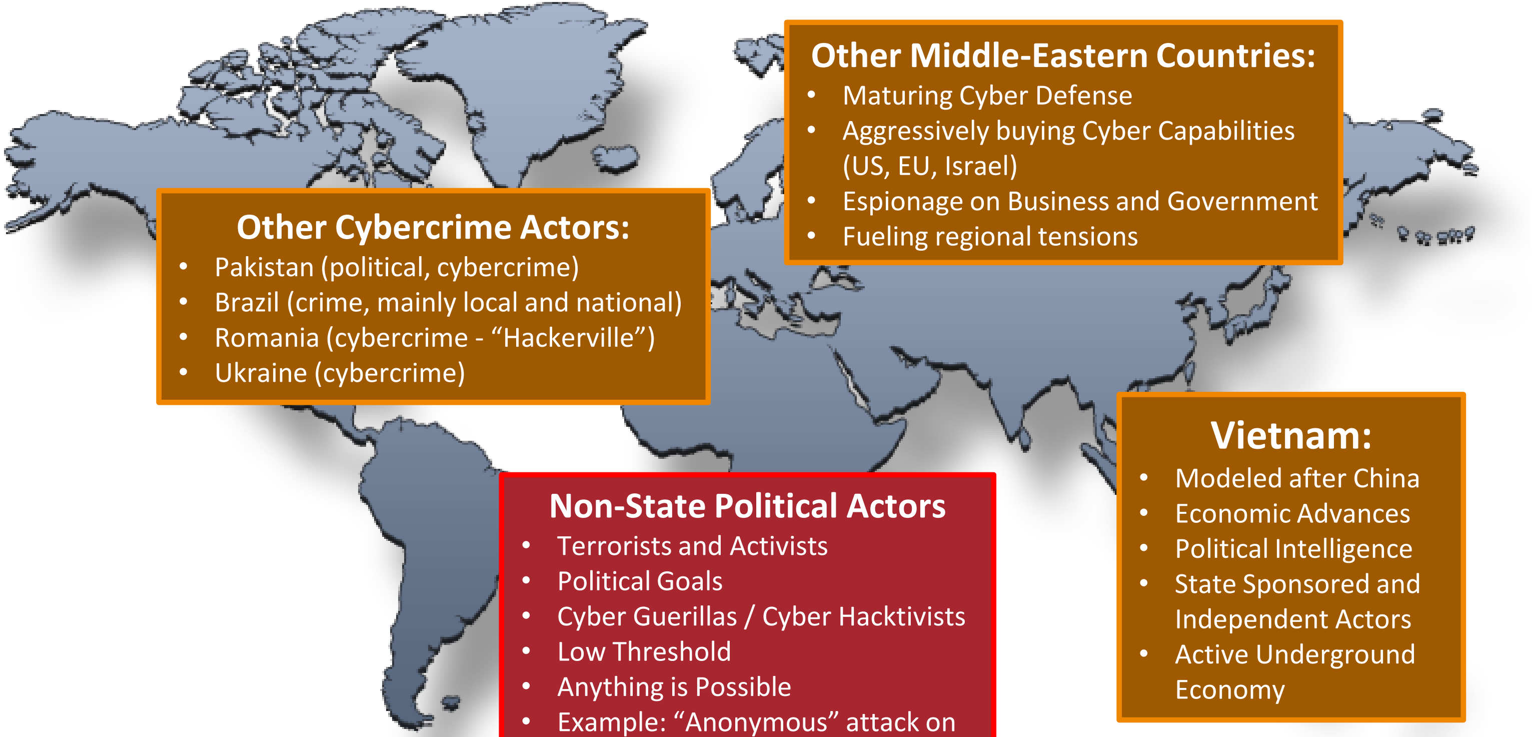
Iran:

- Developed advanced cyber capabilities in response to Stuxnet (2010)
- Highly developed
- Cyber Warfare defensive and offensive capabilities

North Korea:

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

Nation States - the “Up and Coming”



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

Non-State Political Actors

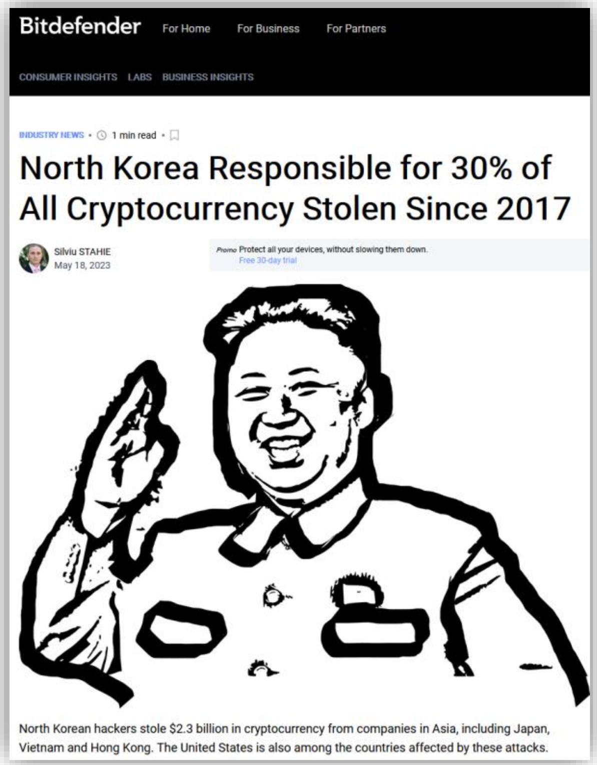
- Terrorists and Activists
- Political Goals
- Cyber Guerillas / Cyber Hacktivists
- Low Threshold
- Anything is Possible
- Example: “Anonymous” attack on Boston Children’s Hospital

Vietnam:

- Modeled after China
- Economic Advances
- Political Intelligence
- State Sponsored and Independent Actors
- Active Underground Economy

PATCH

The World we Live in ….. Nation State Attackers



North Korea Responsible for 30% of All Cryptocurrency Stolen Since 2017

Silviu STAHIE
May 18, 2023

North Korean hackers stole $2.3 billion in cryptocurrency from companies in Asia, including Japan, Vietnam and Hong Kong. The United States is also among the countries affected by these attacks.

Increasing malicious cyber activity by Nation States for varying reasons:

- Financial / economic
- Espionage / intellectual property
- Sabotage
- Political Goals
- Cyber defensive and offensive capabilities

Nation State objectives in cyber space range from improving their own economic situation to support of their political goals and agenda.

https://www.bitdefender.com/blog/hotforsecurity/north-korea-responsible-for-30-of-all-cryptocurrency-stolen-since-2017/

PATCH

The World we Live in ….. Nation State Attackers

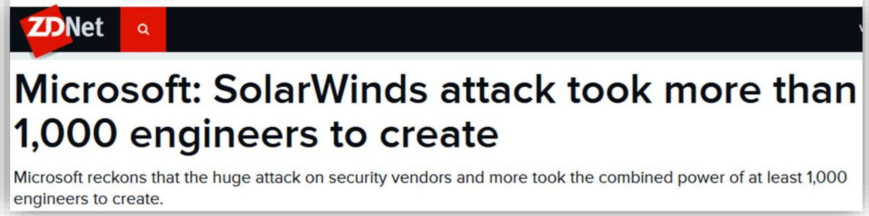
Further information, if interested (not a mandatory reading assignment):

- Analytics Exchange Program (AEP, a public/private partnership): Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar
  https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf
- Aspen Institute Cyber Threat Assessment: the Rise of the Rest: Maturing Cyber Threats Beyond the Big Four
  https://www.aspeninstitute.org/programs/cybersecurity-technology-program/threat-assessment-2019/
- Inside a future cyberwar: What will cyber warfare really be like?
  https://www-deseret-com.cdn.ampproject.org/c/s/www.deseret.com/platform/amp/2021/8/11/22606230/inside-a-future-cyberwar

Example: Advanced Nation State & Cybercriminal Attacks

SolarWinds Attack:

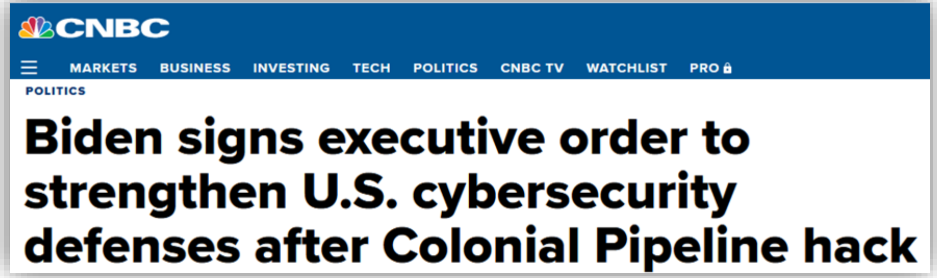
- Months-long hacking campaign, discovered Dec. 2020
- “The largest and most sophisticated attack the world has ever seen“ (Microsoft)
- Sunburst malware inside SolarWinds's Orion network management software
- US government agencies and cybersecurity vendors
- Impacted est. 18,000 organizations
- Microsoft assigned 500 engineers to investigate
- Estimates team that created it was twice the size



Microsoft: SolarWinds attack took more than 1,000 engineers to create

Microsoft reckons that the huge attack on security vendors and more took the combined power of at least 1,000 engineers to create.

https://www.zdnet.com/article/microsoft-solarwinds-attack-took-more-than-1000-engineers-to-create/



Biden signs executive order to strengthen U.S. cybersecurity defenses after Colonial Pipeline hack

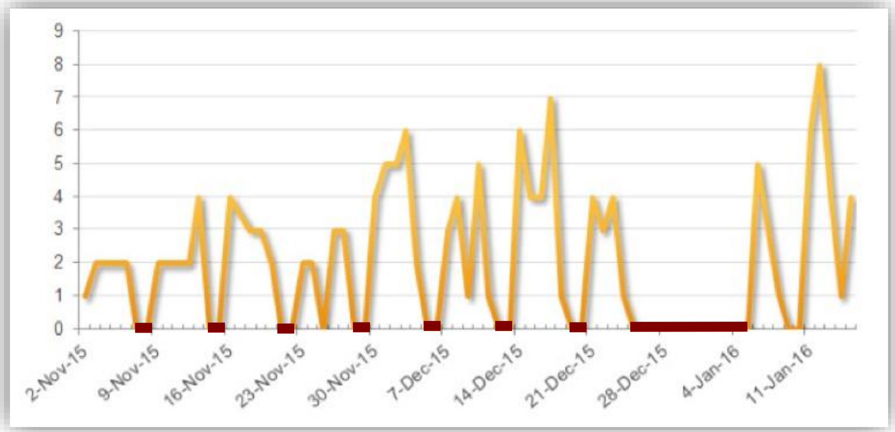
Colonial Pipeline Attack:

- Ransomware led to shutdown of 5,500 miles of pipeline
- Paid $ 4.4m to cybercriminal group DarkSide
- 45% of East Coast fuel supply, widespread shortages
- Got within 3 days of running out of diesel fuel
- “All government response” and Cybersecurity Executive Order as a result of “persistent and increasingly sophisticated malicious cyber campaigns”
- Challenging restart operations
- DarkSide claims that their servers were shut down and moneys were seized

https://www.cnbc.com/2021/05/12/biden-signs-executive-order-to-strengthen-cybersecurity-after-colonial-pipeline-hack.html

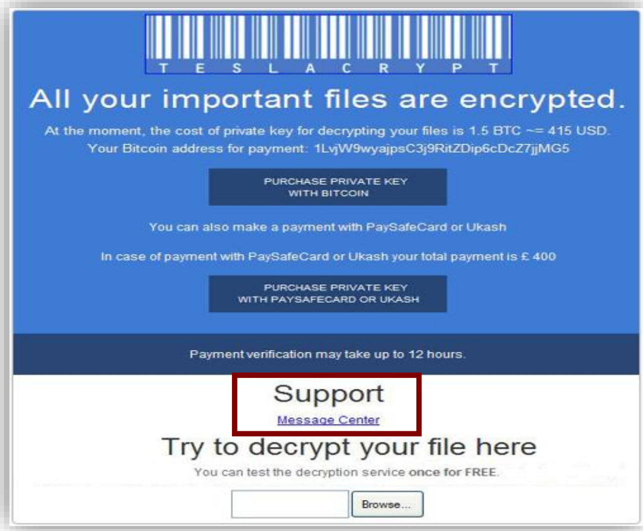
Professionalization of Cybercrime

Dridex Gang – Number of Known Spam Runs Per Day



"2016 Internet Security Threat Report", Symantec Corp.

TeslaCrypt Ransomware – Technical Support Available



All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ~= 415 USD.
Your Bitcoin address for payment: 1LvjW9wyajpsC3j9RitZDip6cDcZ7jjMG5

PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

PURCHASE PRIVATE KEY WITH PAYSAFECARD OR UKASH

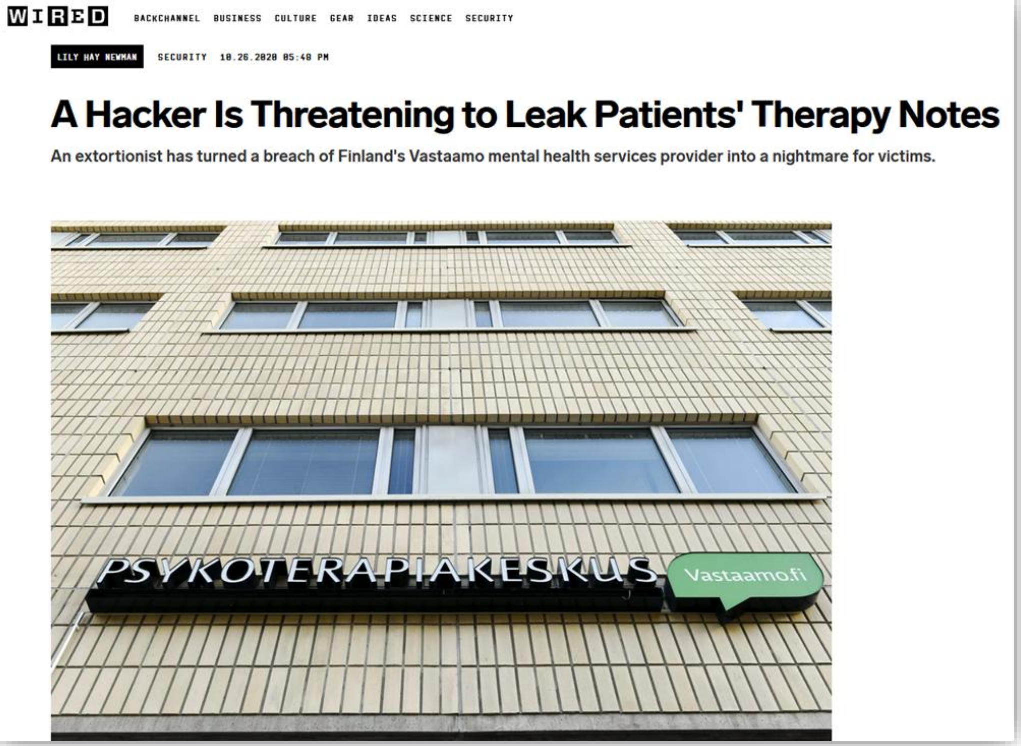
Payment verification may take up to 12 hours.

Support

Try to decrypt your file here

You can test the decryption service once for FREE.

Cybercriminals’ Evolving Business Models



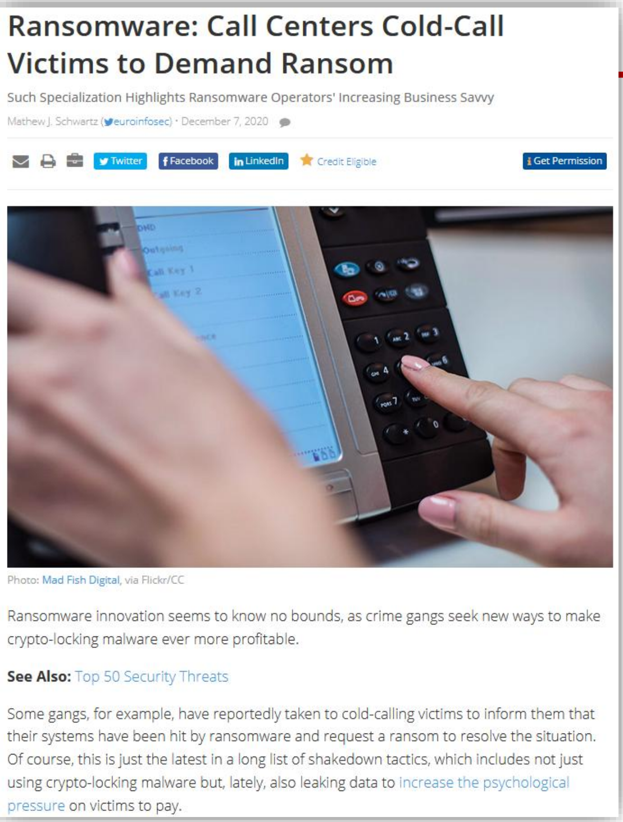
WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

LILY HAY NEWMAN SECURITY 10.26.2020 05:40 PM

A Hacker Is Threatening to Leak Patients' Therapy Notes

An extortionist has turned a breach of Finland's Vastaamo mental health services provider into a nightmare for victims.

https://www.wired.com/story/hacker-threaten-release-therapy-notes-patients/



Ransomware: Call Centers Cold-Call Victims to Demand Ransom

Such Specialization Highlights Ransomware Operators' Increasing Business Savvy

Mathew J. Schwartz (euroinfosec) • December 7, 2020

Photo: Mad Fish Digital, via Flickr/CC

Ransomware innovation seems to know no bounds, as crime gangs seek new ways to make crypto-locking malware ever more profitable.

See Also: Top 50 Security Threats

Some gangs, for example, have reportedly taken to cold-calling victims to inform them that their systems have been hit by ransomware and request a ransom to resolve the situation. Of course, this is just the latest in a long list of shakedown tactics, which includes not just using crypto-locking malware but, lately, also leaking data to increase the psychological pressure on victims to pay.

https://www.healthcareinfosecurity.com/ransomware-call-centers-cold-call-victims-to-demand-ransom-a-15535

Political Cyber Conflicts - a Growing Risk

Growing attack surface – attackers roll with opportunities:

- Digitization (more data)
- Digitalization (more digital infrastructure)
- Technology adoption (IoT, cloud, 5G, AI/ML – see next slide)

New and creative attack vectors:

- Supply Chain as attack vector
- Data in Transit attacks

Consequently:

- We will continue to see big names in the headlines
- It will not just be about *Confidentiality* anymore

FROM THE WESTERN CAPITALIST PIGS WHO BROUGHT YOU NEIGHBORS AND THIS IS THE END
SETH ROGEN JAMES FRANCO
이 무식한 미국놈들을 믿지 마십시오!
THE INTERVIEW
CHRISTMAS

As Threats Evolve - Security Must, 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.
Accompanied by safe roads, signs and signals,
traffic laws, driving tests, and “audits”.

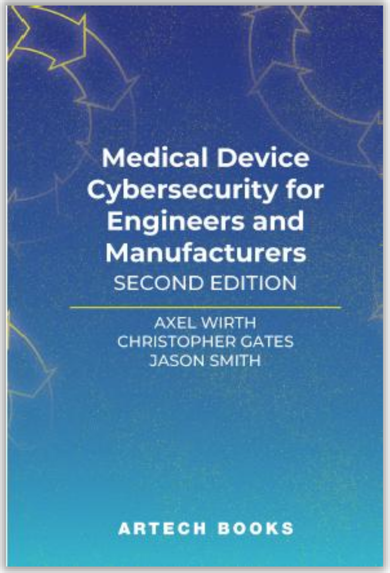
Leave behind your “old security” mindset. Today we need a new approach … and I assume tomorrow again. Protect: Data, infrastructure, operations, and business.

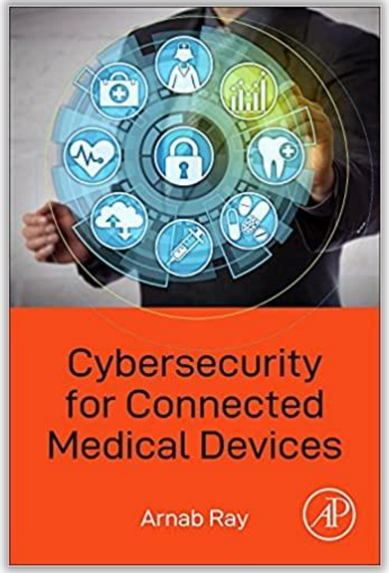
In Cybersecurity, we are operating in non-linear space. Although we can analyze trends and make predictions, any event can turn the status quo on its head.

Thank you!

axel@medcrypt.com

General Resources - For Medical Device Manufacturers

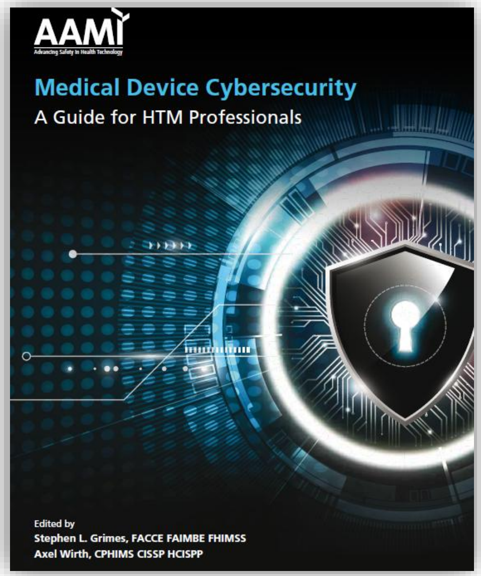


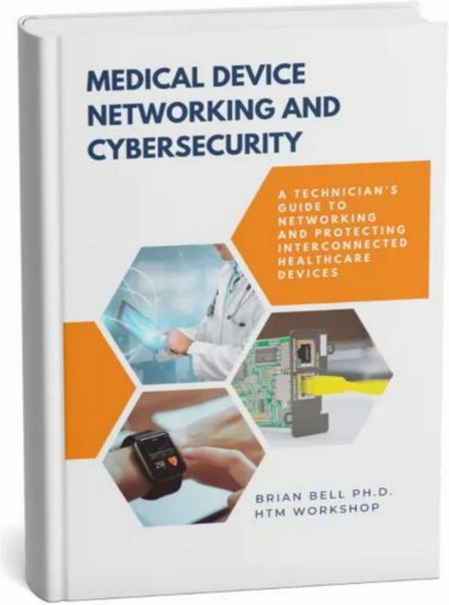


US: https://us.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2416.aspx
UK: https://uk.artechhouse.com/Medical-Device-Cybersecurity-for-Engineers-and-Manufacturers-Second-Edition-P2354.aspx

https://www.amazon.com/Cybersecurity-Connected-Medical-Devices-Arnab/dp/0128182628/ref=sr_1_4

General Resources - For Healthcare Delivery Organization

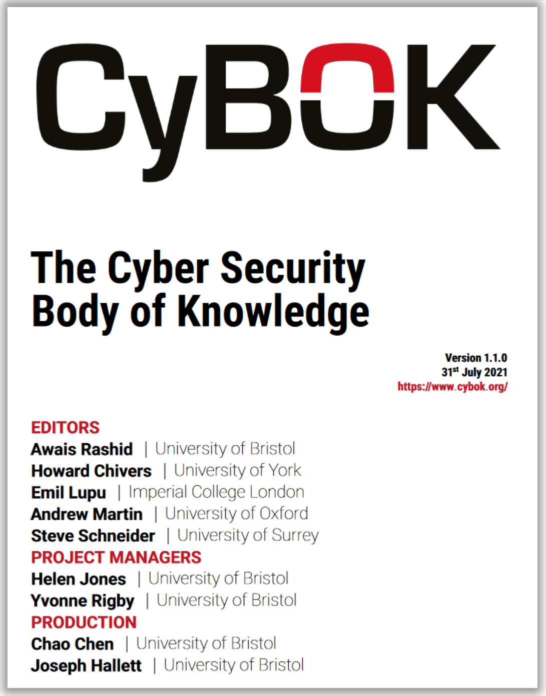

AAMI
Advancing Safety in Health Technology
Medical Device Cybersecurity
A Guide for HTM Professionals
Edited by
Stephen L. Grimes, FACCE FAIMBE FHIMSS
Axel Wirth, CPHIMS CISSP HCISPP


MEDICAL DEVICE NETWORKING AND CYBERSECURITY
A TECHNICIAN'S GUIDE TO NETWORKING AND PROTECTING INTERCONNECTED HEALTHCARE DEVICES
BRIAN BELL PH.D.
HTM WORKSHOP

https://store.aami.org/s/store#/store/browse/detail/a152E000006j66qQAA

https://htm-workshop.com/shop/medical-device-networking-and-cybersecurity/

General Resources - CyBOK



CyBOK

The Cyber Security Body of Knowledge

Version 1.1.0
31st July 2021
https://www.cybok.org/

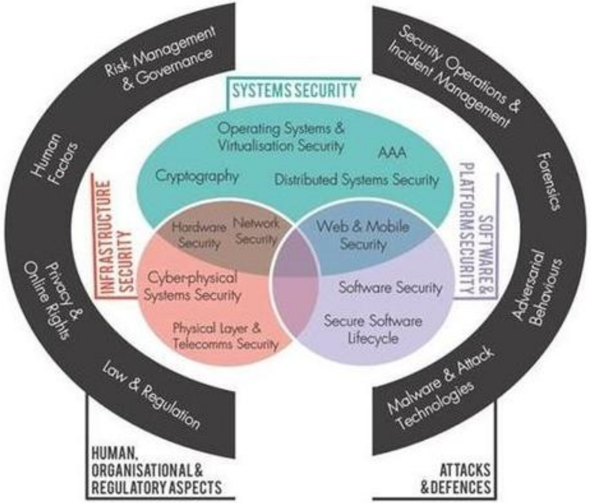
EDITORS
Awais Rashid | University of Bristol
Howard Chivers | University of York
Emil Lupu | Imperial College London
Andrew Martin | University of Oxford
Steve Schneider | University of Surrey

PROJECT MANAGERS
Helen Jones | University of Bristol
Yvonne Rigby | University of Bristol

PRODUCTION
Chao Chen | University of Bristol
Joseph Hallett | University of Bristol

The Cyber Security Body of Knowledge v1.1, https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

CyBOK Knowledge Base https://www.cybok.org/knowledgebase1_1/


Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
AAA
Cryptography
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Web & Mobile Security
Cyber-physical Systems Security
Software Security
Physical Layer & Telecomms Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

Staying Informed on the Day-to-Day

- Security briefs and threat alerts via Health Sector Cybersecurity Coordination Center (HC3) https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html
- US Department of Homeland Security's Industrial Control Systems—Cyber Emergency Response Team (ICS-CERT) medical device alerts (ICSMA) https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A96
- Healthcare and Public Sector Highlights - Cybersecurity (via HHS) https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare
- CISA HPH Sector https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector