unicri
United Nations
Interregional Crime and Justice
Research Institute

Cybersecurity in the Healthcare Sector

19 June 2017

Francesca Bosco, UNICRI

Presentation Overview

- Cyber-Related Innovations in Healthcare
- The Current Cybersecurity Threat Landscape
- Case study: WannaCry
- Case study: Pacemaker hacking
- Case study: Hacking robots
- Challenges
- Conclusions

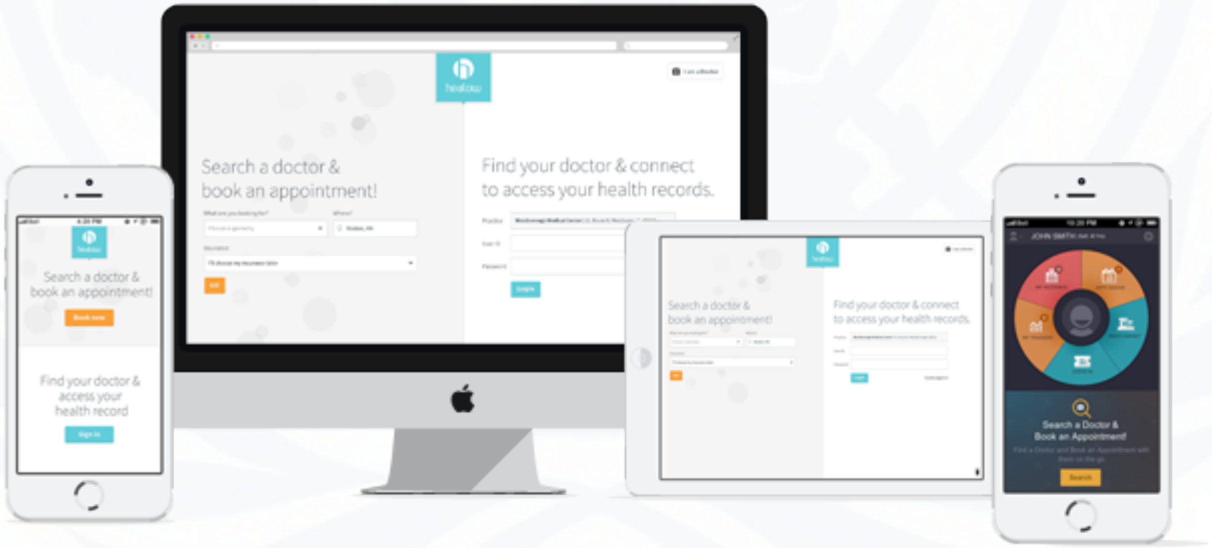
Cyber-Related Innovations in Healthcare

- The adoption of **cloud computing** for digital management of medical records
- Spending on cloud computing is estimated to reach $1 trillion between now and 2022

(Schwartz 2017)

Cyber-Related Innovations in Healthcare

- **Cloud computing** also allows for greater interaction between patients and their healthcare providers



Search a doctor & book an appointment!

Find your doctor & connect to access your health records.

Find your doctor & access your health record

Search a Doctor & Book an Appointment!

(Schwartz 2017)

Cyber-Related Innovations in Healthcare

- The development of **advanced computerized devices, implants,** and **smart prostheses**

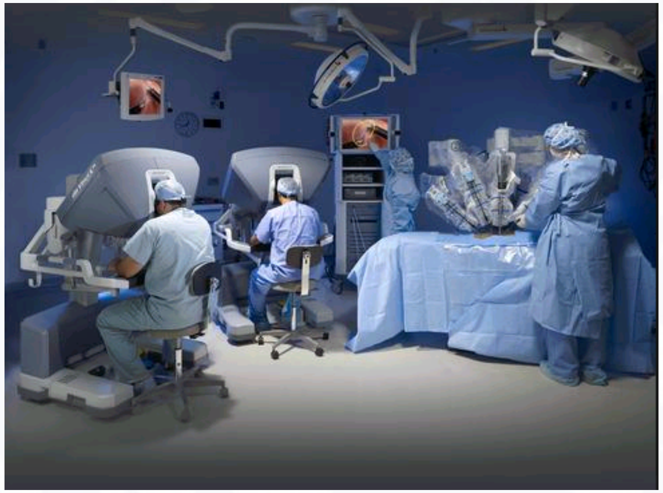
Merlin@home™

Massimo MultiSAT™

Bionic or "Smart" prostheses

(Schwartz 2017)

Robots in Healthcare



Da Vinci

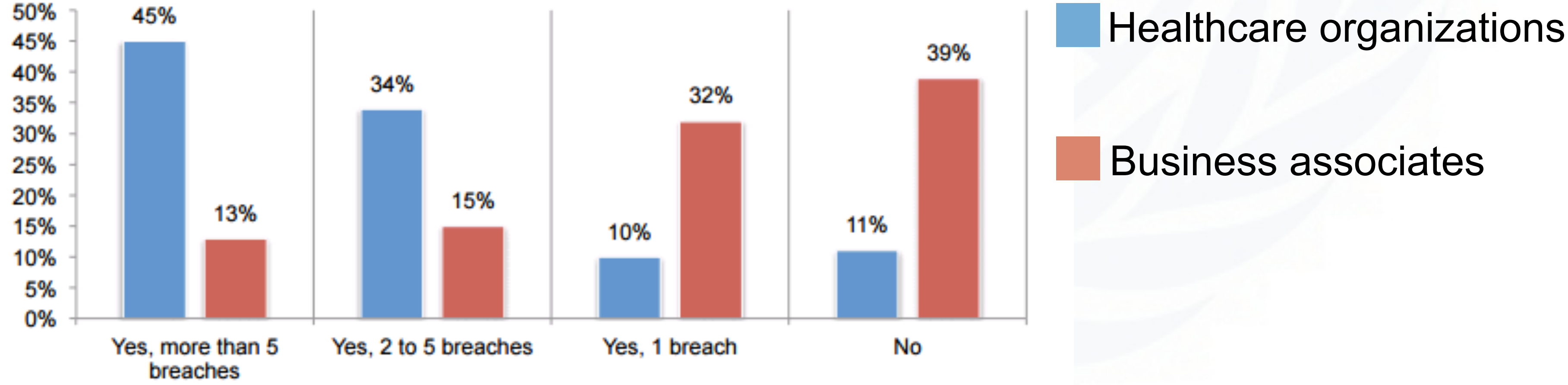
The Tug

DENSO

The Current Cybersecurity Threat Landscape

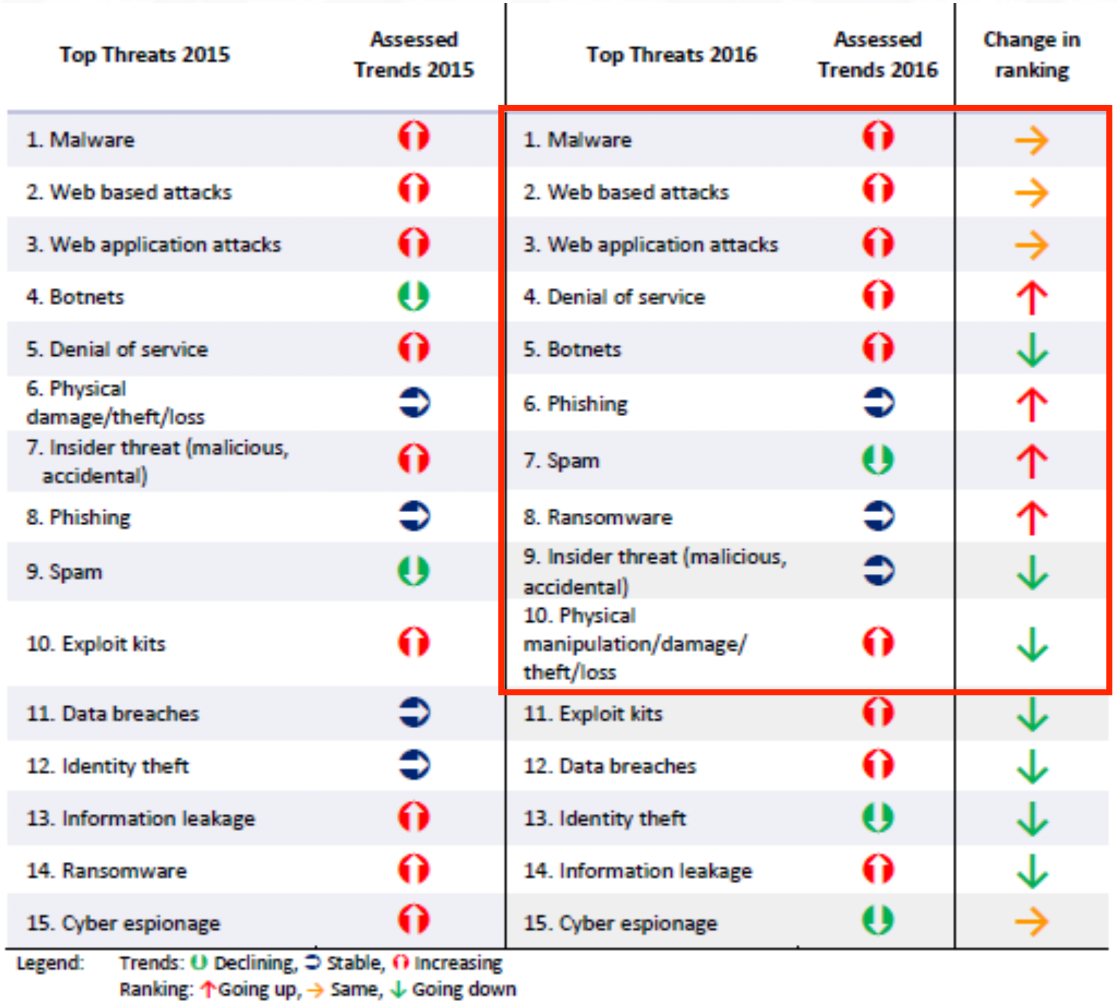
- These innovations have increased the quality of care, but they have also introduced **new cybersecurity threats** into the existing threat landscape
- As a result, the healthcare industry is an **increasingly attractive target** for cybercriminals

Figure 14. Has your organization suffered a data breach involving the loss or theft of patient data in the past 24 months?



(Ponemon Institute 2016)

The Current Cybersecurity Threat Landscape



Top Threats 2015	Assessed Trends 2015	Top Threats 2016	Assessed Trends 2016	Change in ranking
1. Malware	⇧	1. Malware	⇧	→
2. Web based attacks	⇧	2. Web based attacks	⇧	→
3. Web application attacks	⇧	3. Web application attacks	⇧	→
4. Botnets	⇩	4. Denial of service	⇧	↑
5. Denial of service	⇧	5. Botnets	⇧	↓
6. Physical damage/theft/loss	⇨	6. Phishing	⇨	↑
7. Insider threat (malicious, accidental)	⇧	7. Spam	⇩	↑
8. Phishing	⇨	8. Ransomware	⇨	↑
9. Spam	⇩	9. Insider threat (malicious, accidental)	⇨	↓
10. Exploit kits	⇧	10. Physical manipulation/damage/ theft/loss	⇧	↓
11. Data breaches	⇨	11. Exploit kits	⇧	↓
12. Identity theft	⇨	12. Data breaches	⇧	↓
13. Information leakage	⇧	13. Identity theft	⇩	↓
14. Ransomware	⇧	14. Information leakage	⇧	↓
15. Cyber espionage	⇧	15. Cyber espionage	⇩	→

Legend: Trends: ⇩ Declining, ⇨ Stable, ⇧ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

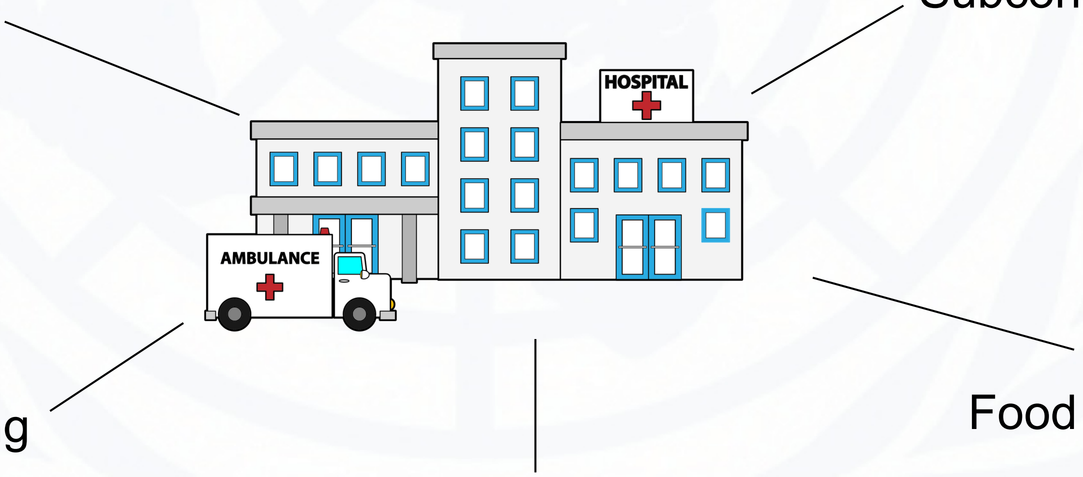
Figure 1: Overview and comparison of the current threat landscape 2016 with the one of 2015[1].

Top 10 Threats, 2016

(European Union Agency for Network and Information Security 2016)

The Current Cybersecurity Threat Landscape

- Keep in mind that cybersecurity threats to the healthcare industry can target **the supply chain** as an entry point



Vendors

Subcontractors

Air conditioning services

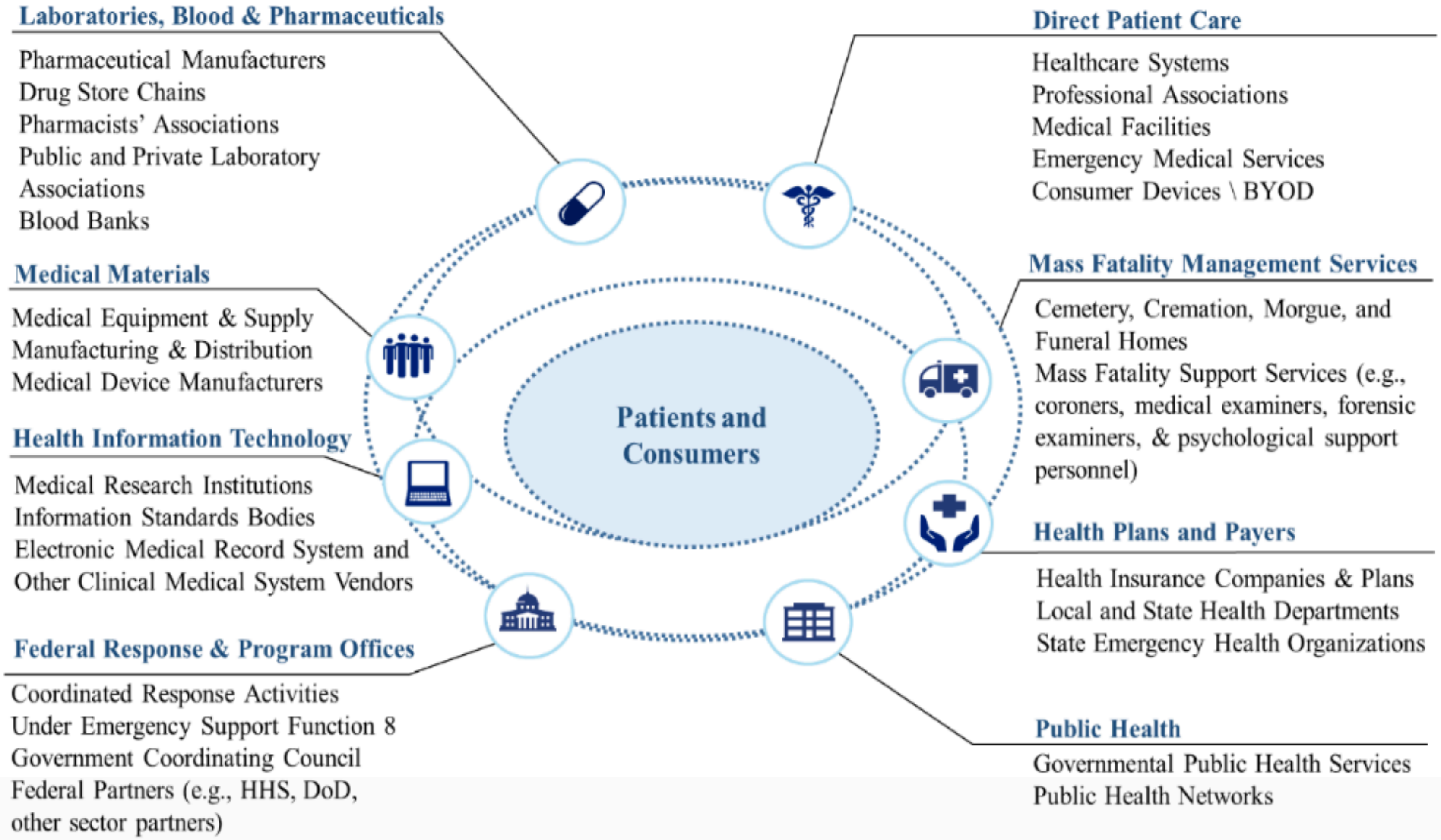
Cloud services

Food services

(Digital Guardian 2017)

The Current Cybersecurity Threat Landscape

Figure 2 Health Care Ecosystem



Patients and Consumers

Laboratories, Blood & Pharmaceuticals

Pharmaceutical Manufacturers
Drug Store Chains
Pharmacists' Associations
Public and Private Laboratory Associations
Blood Banks

Medical Materials

Medical Equipment & Supply Manufacturing & Distribution
Medical Device Manufacturers

Health Information Technology

Medical Research Institutions
Information Standards Bodies
Electronic Medical Record System and Other Clinical Medical System Vendors

Federal Response & Program Offices

Coordinated Response Activities Under Emergency Support Function 8
Government Coordinating Council
Federal Partners (e.g., HHS, DoD, other sector partners)

Direct Patient Care

Healthcare Systems
Professional Associations
Medical Facilities
Emergency Medical Services
Consumer Devices \ BYOD

Mass Fatality Management Services

Cemetery, Cremation, Morgue, and Funeral Homes
Mass Fatality Support Services (e.g., coroners, medical examiners, forensic examiners, & psychological support personnel)

Health Plans and Payers

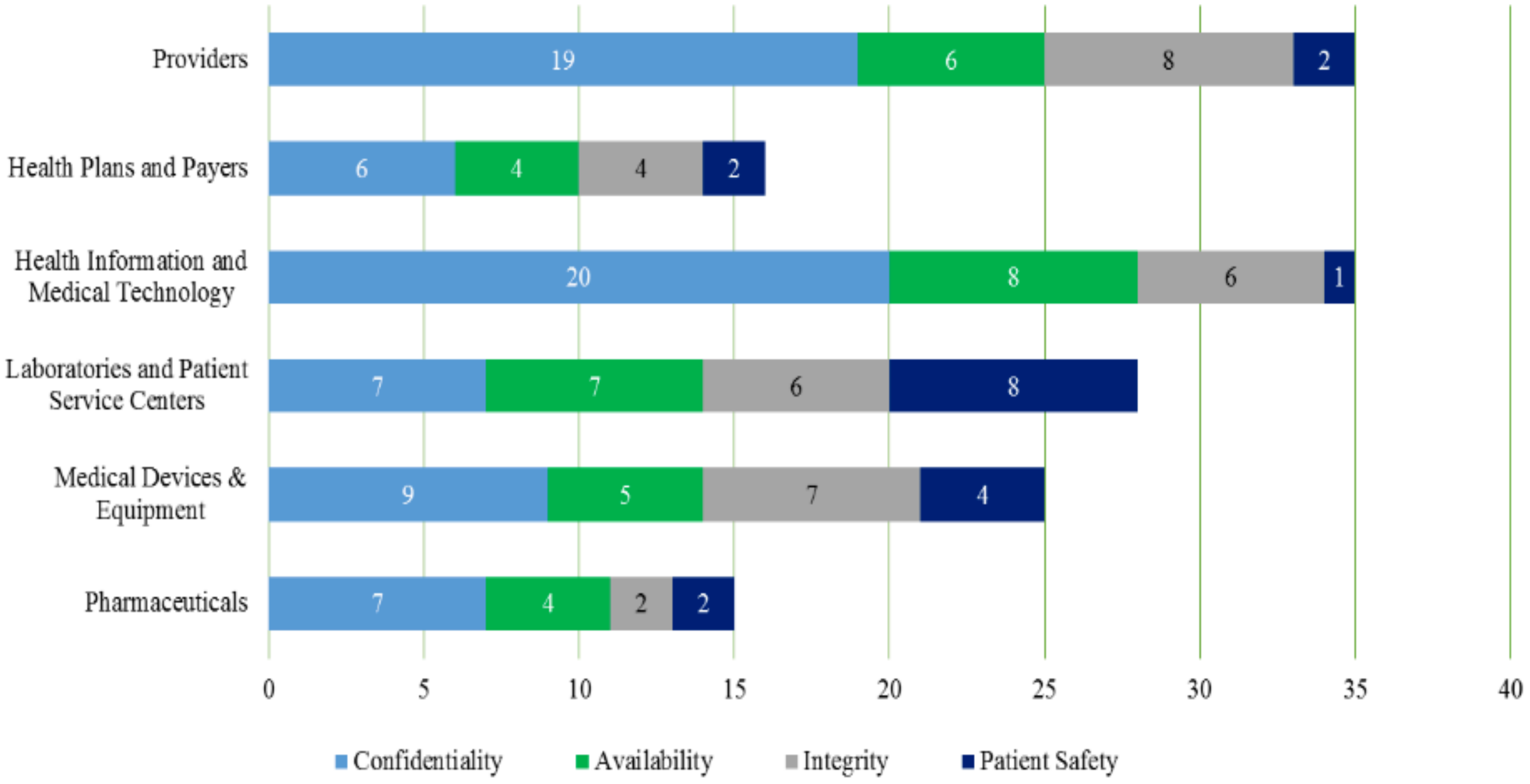
Health Insurance Companies & Plans
Local and State Health Departments
State Emergency Health Organizations

Public Health

Governmental Public Health Services
Public Health Networks

The Current Cybersecurity Threat Landscape

Figure 4 Health Care Subsector Risks across the Value Chain



The Current Cybersecurity Threat Landscape

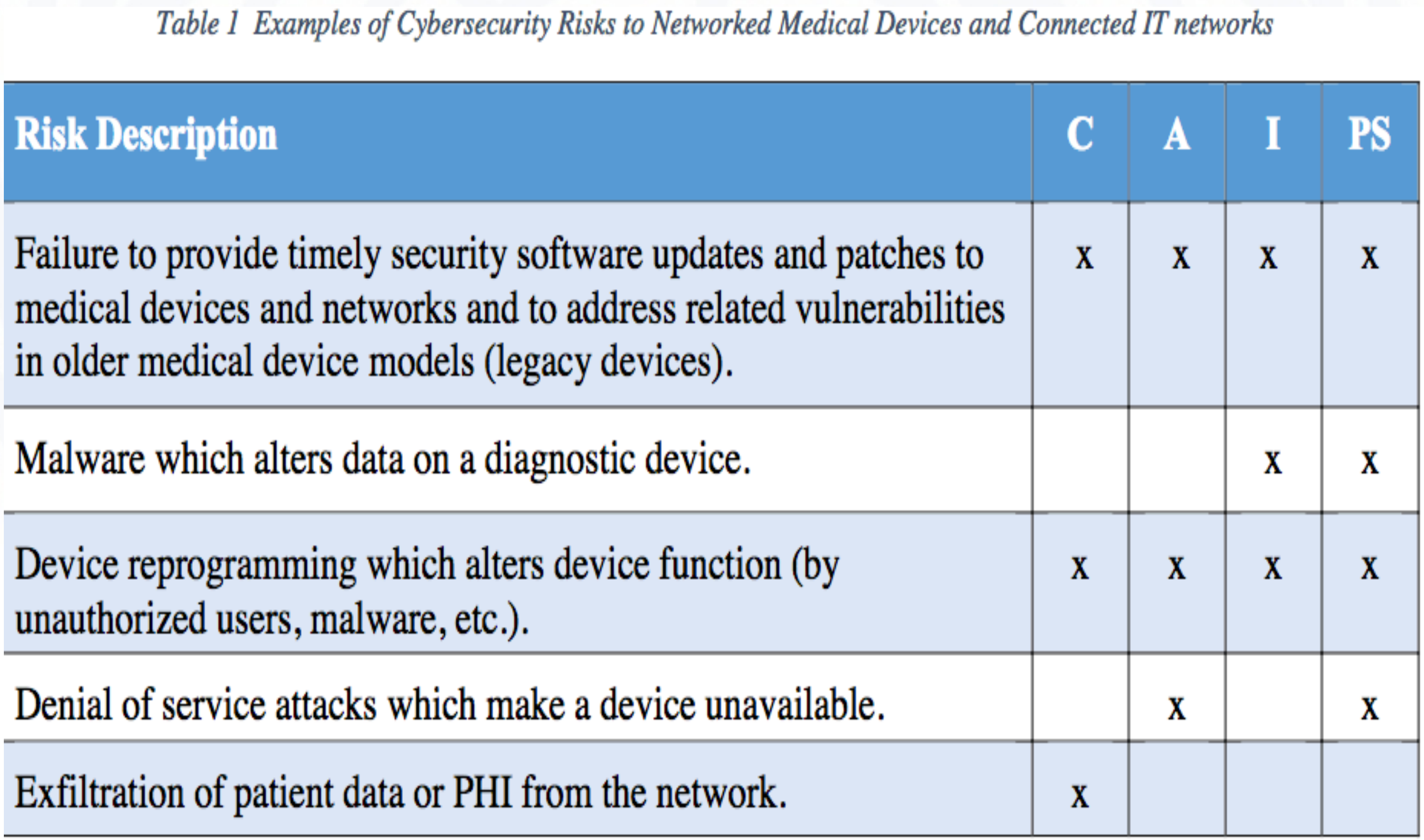
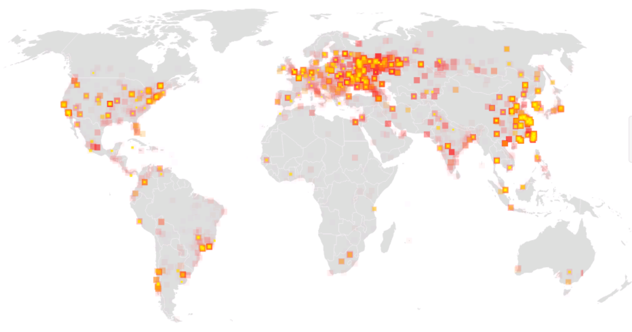


Table 1 Examples of Cybersecurity Risks to Networked Medical Devices and Connected IT networks

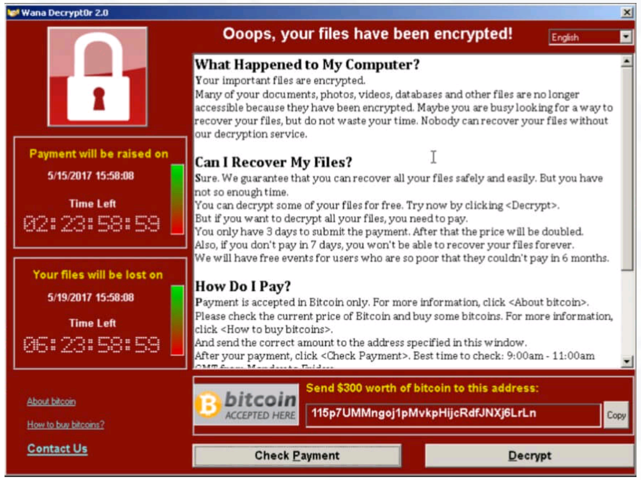
Risk Description	C	A	I	PS
Failure to provide timely security software updates and patches to medical devices and networks and to address related vulnerabilities in older medical device models (legacy devices).	x	x	x	x
Malware which alters data on a diagnostic device.			x	x
Device reprogramming which alters device function (by unauthorized users, malware, etc.).	x	x	x	x
Denial of service attacks which make a device unavailable.		x		x
Exfiltration of patient data or PHI from the network.	x			

The Current Cybersecurity Threat Landscape

- Ransomware Case Study: **WannaCry**



- Date: May 2017
- Number of impacted countries: 150
- Number of impacted systems: 230,000



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 15:58:08
Time Left
02:23:58:59

Your files will be lost on
5/19/2017 15:58:08
Time Left
06:23:58:59

Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

(European Union Agency for Network and Information Security 2016)

The Current Cybersecurity Threat Landscape

- Hacking Case Study: **Pacemakers**

- Researchers have been able to:
  - Steal owner's personal information from the pacemaker
  - Turn off pacemaker entirely
  - Remotely control pacing

"I realized my heart was now **wired into the medical Internet of Things**, and this was done without informing me or asking for my consent. I recognized right away that this remote monitoring capability is very beneficial to a lot of patients who require frequent check-ups, but **with connectivity comes vulnerability**." – Marie Moe

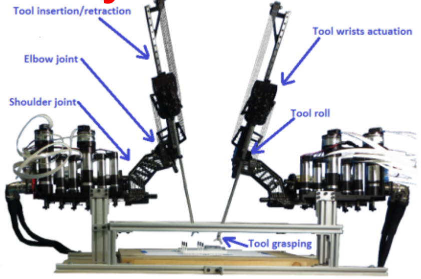
(Wired 2016)

The Current Cybersecurity Threat Landscape

- Hacking Case Study: **Robots**

  - Researchers from the University of Washington – Seattle have been able to hack into a teleoperated surgical robot in an attempt to test the device’s security framework.

  - Researchers were able to hack the Raven II robot, which was running the Interoperable Telesurgery Protocol. This communication interface links the surgeon’s PC with the telerobot on the open Internet, making surgeries possible in hardship locations, but also posing security risks.



Challenges and Solutions

- The law is always playing catch-up with technology. How can the law keep up with constant innovations?
- How to make sure existing laws do not hinder technological developments?
- Balancing act between allowing new technological innovation without endangering the health, safety, rights, and values of people

----

- Soft law: technical and safety norms and standards; professional associations; codes of conduct
- Responsible research and innovation
- Smart regulation
- No obsolete systems

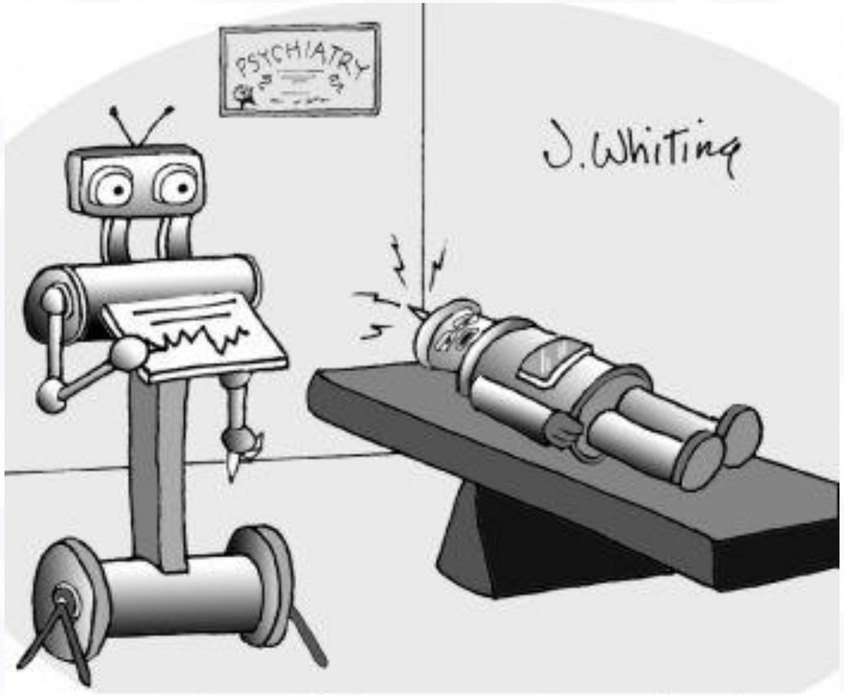
Conclusions

- Innovation and adoption of new technologies in the healthcare sector has the capacity to increase efficiency and quality of care

HOWEVER...

- It must coincide with careful considerations about keeping networks, devices, and supply chains secure.

Questions?



“It’s hard for me to admit this, but I was hacked.”

Contact Information

Francesca Bosco

Project Officer

bosco@unicri.it

@francibosco

UNICRI:

http://unicri.it/special_topics/securing_cyberspace/