

Human Factor in IT-Security within the medical context

2nd Bridging the Gap Workshop

24.05.2022

Stefan Sütterlin

Recent developments

- “Smart” medical devices (ICDs/pacemakers, infusion pumps, MRI machines) enable connectivity and incorporate software.
- Software needs to be maintained, updated, i.e., has interfaces.
- Software with interface creates cyber vulnerability.
- In an increasing number of cases medical devices were recalled following weaknesses discovered by government security entities and academic institutions.



(2019)

Cybersecurity Vulnerabilities Affecting Medtronic Implantable Cardiac Devices, Programmers, and Home Monitors: FDA Safety Communication

EDITORIAL COMMENTARY

Striking the right balance when addressing cybersecurity vulnerabilities

William H. Maisel, MD, MPH, Jessica E. Paulsen, BE, Matthew B. Hazelett, BS,
Kimberly A. Selzman, MD, MPH, FHRS

From the U.S. Food and Drug Administration, Silver Spring, Maryland.


We recognize the importance of striking the right balance between **advancing device cybersecurity and avoiding unnecessary anxiety and inconvenience** for patients and their health care providers.

(...)

However, we are also committed to **preventing a widespread cybersecurity incident that could have important public health consequences**. Recent experience with software deployments for CIEDs has demonstrated that there is **variability among the clinical community in the implementation of cybersecurity updates** for these devices.

The novelty of these issues and the **misconception that cybersecurity risks are theoretical** may have contributed to the variable and inconsistent approach to handling these updates.

Remote programming of cardiac implantable electronic devices: A novel approach to program cardiac devices for magnetic resonance imaging

Sisir Siddamsetti MD  | Alexander Shinn DO, MBA | Sandeep Gautam MD, MPH, FHRS

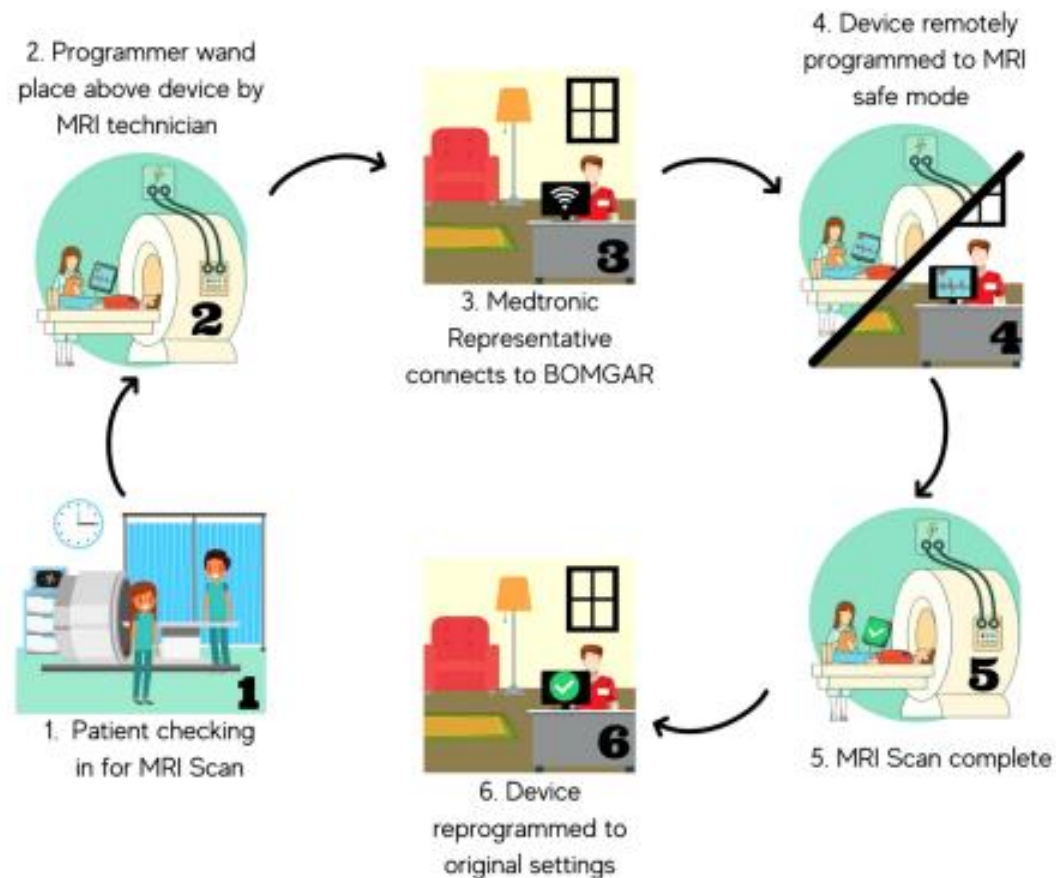
Abstract

Background: Magnetic resonance imaging (MRI) in patients with MRI-conditional cardiovascular implantable electronic devices (CIED) remain a logistical issue for device programming during the scan. In current practice, a trained person needs to be present on-site to program CIED for MRI scan. This can cause delay in patient care, rescheduling of tests and increase healthcare costs. A novel remote programming (RP) strategy can be utilized to reprogram the CIED remotely. We sought to explore the feasibility and safety of RP of CIEDs in patients undergoing MRI scan.

Methods: We implemented the Medtronic CIED RP software at our institution after ensuring HIPAA compliance. The MRI technician started the session by contacting an off-site remote operator and placing a programmer wand from the 2090 Medtronic programmer over the CIED. The remote operator logged into a remote access software and provided a unique access code to the MRI technician. After entering the access code into the programmer, the remote operator was able to program the device as needed. We conducted a periodic audit of the first 209 patients who underwent RP of CIEDs for MRI. Outcomes analyzed were successful completion of RP sessions and time saved per scan.

Results: Of the 209 MRI scans, 51 scans were performed urgently. There were no connectivity and programming problems or need for MRI rescheduling. In-person reprogramming was not required for any patient. All scans were completed safely in a timely manner, and there were no reports of CIED malfunction. Time saved per scan was estimated to be 28 ± 10 min.

Conclusions: Remote programming of CIEDs for MRI scans is a safe and effective strategy.



programming the device remotely. This study and others may raise legitimate concerns about the susceptibility of CIEDs to remote hacking via gaps in cybersecurity,^{17,18} particularly considering previously known data breaches in electronic medical records of a majority of healthcare organizations.¹⁹ In recent years, there have been some cybersecurity concerns with regards to multiple vendors.²⁰ Specifically, in 2018, FDA issued a security update about the Medtronic CareLink programmers (CareLink 2090 and CareLink Encore 29901) regarding Medtronic Software Deployment Network (SDN) which is used to obtain software updates over the internet,²¹ due to concerns about allowing unauthorized users to upload software onto the programmers. In-response, Medtronic temporarily disabled over the internet software updates using SDN to the programmers and allowed the updates to take place only through the USB port of the programmer until the above-mentioned cybersecurity concern was appropriately addressed. We adopted all the standard measures to maintain stringent cybersecurity such as secure passwords to log in to the programmer device, the remote device used to connect to the programmer and the remote-control software, encryption of data and randomly generated unique session codes for separate programming sessions. Other active and proposed methods to eliminate this risk include limiting of programmer & CIED sales at online auction sites, requiring cybersecurity & testing in premarket development and limiting access to programmers and device information in outpatient clinics.¹⁹

Cybersecurity for Cardiac Implantable Electronic Devices

What Should You Know?

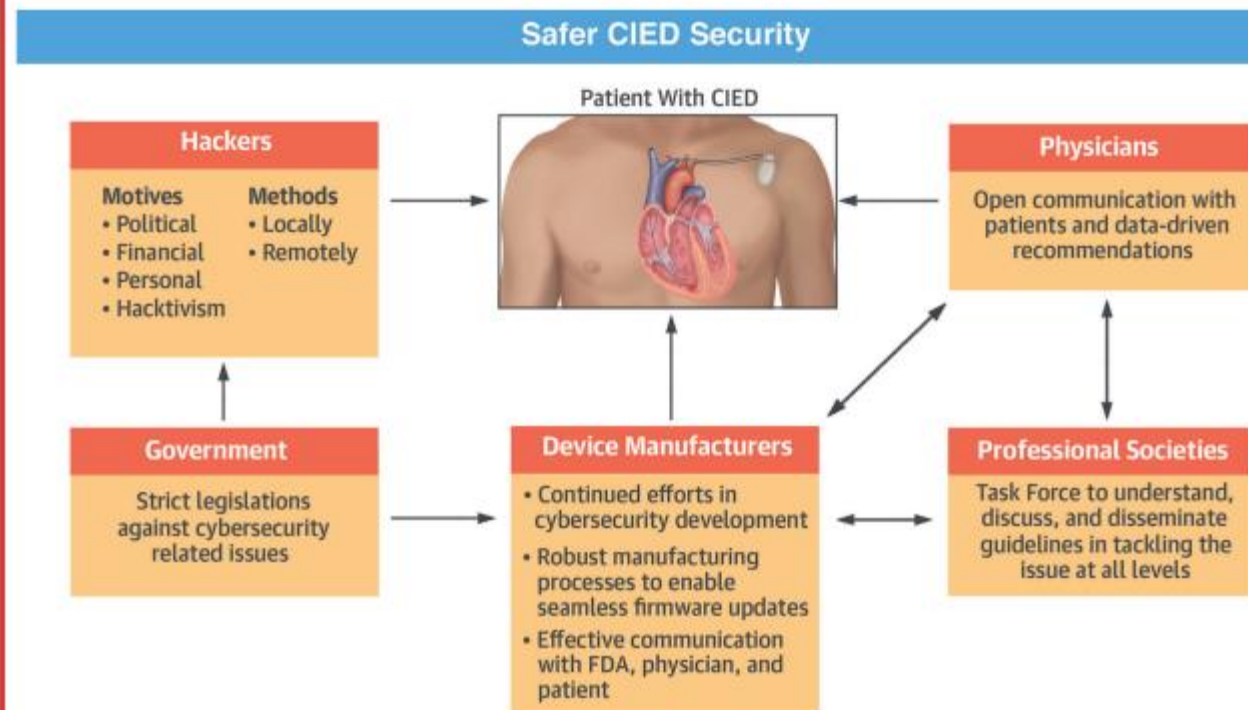
Adrian Baranchuk, MD,^a Marwan M. Refaat, MD,^b Kristen K. Patton, MD,^c Mina K. Chung, MD,^d Kousik Krishnan, MD,^e Valentina Kutiyfa, MD, PhD,^f Gaurav Upadhyay, MD,^g John D. Fisher, MD,^h Dhanunjaya R. Lakkireddy, MD,ⁱ from the American College of Cardiology's Electrophysiology Section Leadership

ABSTRACT

Medical devices have been targets of hacking for over a decade, and this cybersecurity issue has affected many types of medical devices. Lately, the potential for hacking of cardiac devices (pacemakers and defibrillators) claimed the attention of the media, patients, and health care providers. This is a burgeoning problem that our newly electronically connected world faces. In this paper from the Electrophysiology Section Council, we briefly discuss various aspects of this relatively new threat in light of recent incidents involving the potential for hacking of cardiac devices. We explore the possible risks for the patients and the effect of device reconfiguration in an attempt to thwart cybersecurity threats. We provide an outline of what can be done to improve cybersecurity from the standpoint of the manufacturer, government, professional societies, physician, and patient. (J Am Coll Cardiol 2018;71:1284-8) © 2018 by the American College of Cardiology Foundation.



CENTRAL ILLUSTRATION Interaction Amongst Various Stake Holders in Addressing the Cybersecurity Issue



Baranchuk, A. et al. J Am Coll Cardiol. 2018;71(11):1284-8.

CIED = cardiovascular implantable electronic device; FDA = Food and Drug Administration.



ELSEVIER

Contents lists available at [ScienceDirect](#)

Trends in Cardiovascular Medicine

journal homepage: www.elsevier.com/locate/tcm



Are implanted electronic devices hackable?☆

Bryce Alexander, BSc, MD, Sohaib Haseeb, BSc, Adrian Baranchuk, MD, FACC, FRCPC, FCCS*

Division of Cardiology, Queen's University, Kingston, Ontario, Canada



ARTICLE INFO

Keywords:

Pacemaker
Cybersecurity
Implanted electronic devices

ABSTRACT

Medical devices have become increasingly connected in recent years. While this added interconnectivity has provided capabilities for wireless communication and remote monitoring, it has also introduced possible risks for cybersecurity vulnerabilities. Lately, there has been an increased awareness of the potential for cybersecurity breaches in implanted cardiac devices (pacemakers and defibrillators) among patients, healthcare providers, and the media. In this article, we review the current perspective on cybersecurity in implanted medical devices, including a recent high-profile case example of a cybersecurity threat. We outline the actions taken by all the involved stakeholders in response to the disclosure of potential vulnerabilities in medical devices and summarize the positions of major societies in response to these events.

Published by Elsevier Inc.

“It is important for physicians to be knowledgeable about the risks in this field, as well as the steps that can be taken to mitigate these risks, so they can provide effective and accurate advice to their patients”

Cybersecurity threats to cardiac implantable devices: room for improvement

Emrie Tomaiko and Michael S. Zawaneh

Purpose of review

For over a decade, vulnerabilities in the healthcare industry have been identified. Medical devices such as cardiovascular implantable electronic devices (CIEDs) are particularly concerning because of direct threats to patient safety and protected health information (PHI). Although these vulnerabilities have been identified and changes have been made, there is significant room for improvement. We identify changes and improvements to be made in the industry, by providers, and by patients.

Recent findings

Cybersecurity threats in cardiac implantable devices are legitimate concerns for patient safety and PHI. Changes to cybersecurity in these devices have been made, but are far from sufficient.

Summary

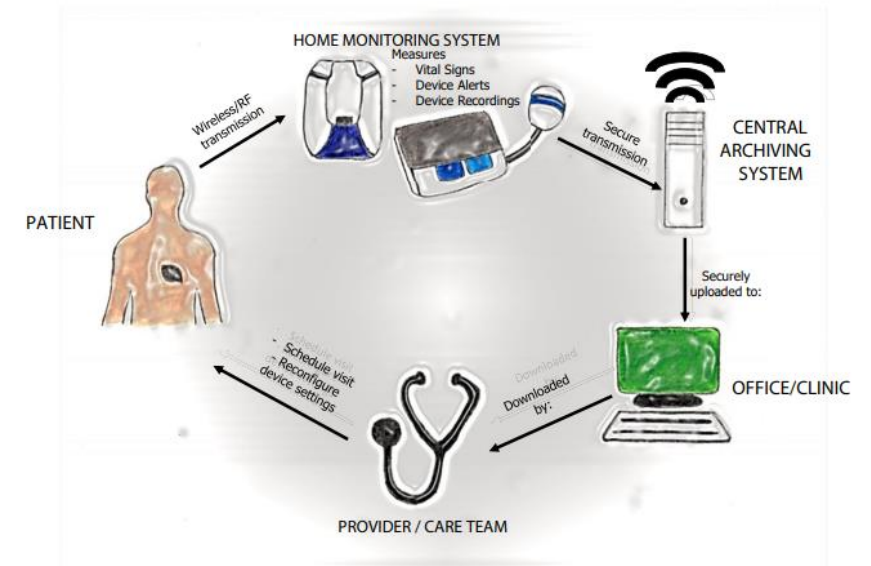
The number of CIEDs implanted worldwide are expected to increase over the next decade. As computer technology advances, cybersecurity threats will only continue to evolve and become more complex. The healthcare industry should seriously consider improvements to protect patients and providers.

Keywords

cardiac implantable devices, cardiovascular implantable electronic devices, cybersecurity, healthcare cybersecurity

KEY POINTS

- The healthcare field, including CIEDs, are vulnerable to cybersecurity attacks.
- Patients tend to express concern about possible attacks affecting the function of their devices, which have only been demonstrated in a research environment.
- Healthcare should educate both patients and themselves regarding cybersecurity risks.
- Physicians should take these risks seriously and take appropriate preventive action.

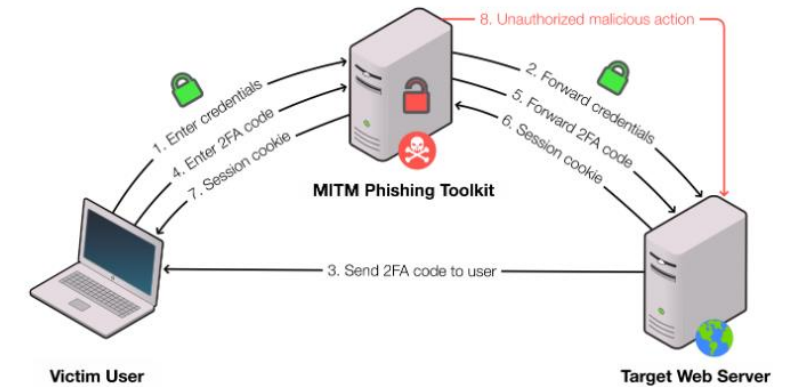


MiTM Phishing Attacks that Bypass 2FA Are on The Rise

Table 1 Attack scenarios, vulnerability explored, and possible harm done

Attack scenario	Vulnerability explored/technique used	Possible harm
CIED-monitor communication interception	Intercepting RF signal with SDR	Stealing patient information Interrupting data transmission to home monitor Inserting wrong data into home monitor, jeopardizing data fidelity Stealing patient information Inserting wrong data into home monitor, jeopardizing data fidelity
Extraction of health data stored in monitor	Connecting to debugging ports MITM attacks during communication between monitor and central server	Stealing patient information Inserting wrong data into home monitor, jeopardizing data fidelity
Insertion of malware into monitor	MITM attack during firmware update Connecting to debugging ports	Causing dysfunction of the monitor Creating a backdoor to steal CIED data Disabling periodic data transmission between the monitor and central server, thus delaying timely recognition of life-threatening CIED recordings
Reading into monitor file system	Connecting to USB port and accessing unencrypted drives on the monitor	Stealing patient information Corrupting file systems and rendering the monitor nonfunctional Deleting stored data Changing stored data and affecting data fidelity Corrupting transmission protocols, rendering talk between the monitor and central server ineffective
Introduction of calibration error in the CIED	Injecting malware through RF commands, especially during home monitor-CIED interaction via the CIED or programmer	Inappropriate reading of patient rhythms Blocking delivery of lifesaving treatments to the patient Decreasing device longevity by draining the battery
Keeping CIED telemetry session open indefinitely	Sending repeated RF signal using SDR	
Insertion of malware into CIED	Sending unauthorized RF signals using SDR MITM attack during CIED-programmer communication	Inserting a faulty algorithm that can prevent appropriate shock or cause inappropriate shock to the patient, causing harm Stealing patient rhythm data Creating a backdoor into the CIED that can be exploited during future attacks
CIED-programmer communication interception	Intercepting RF signals with SDR	Stealing patient information Interrupting data transmission to home monitor Inserting wrong data into programmer, jeopardizing data fidelity Inserting malware into CIED during communication Inserting faulty algorithms and treatment protocols into CIED that can cause patient harm/death
Reading into programmer file system	Intercepting communication between programmer and central server, especially during firmware update process Using USB port or debugging port to read unencrypted files on the programmer memory	Stealing patient information Interrupting data transmission between the programmer and central server Exploiting root access and directory access, injecting malware into the programmer
Insertion of malware into programmer	MITM attack during update session Accessing USB or debugging port	Stealing patient information Keeping a backdoor open for future attacks Injecting faulty algorithms that can be later transmitted to the CIED and cause patient harm
Unauthorized access to cloud server	Exploring DDoS attack Sending malicious http server request	Causing programmer reading errors, making the device nonfunctional Massive data breach with potential to affect thousands of patients

CIED = cardiac implantable electronic device; DDoS = distributed denial of service; MITM = man in the middle; RF = radiofrequency; SDR = software-defined radio; USB = universal serial bus.



[Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits \(catching-transparent-phish.github.io\)](https://catching-transparent-phish.github.io)

Currently, 1200 phishing tool-kits are available in the Darknet.
Some do not or hardly require any IT-skills.

Multiple risk factors

- Authentication
- Privileges and authorization
- Remote access, interfaces
- Maintenance and updates/patches
- ...

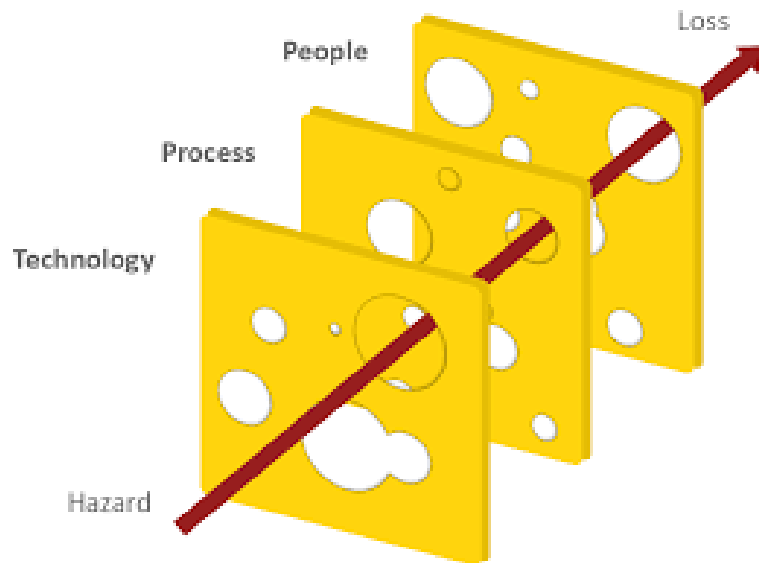
• The number of breach incidents by source:

- Malicious outsider – 56%
- Accidental loss – 34%
- Malicious insider – 7%
- Hacktivist – 2%
- Unknown – 1%

98% of cyber attacks rely on social engineering.

43% of the IT professionals said they had been targeted by social engineering schemes in the last year.

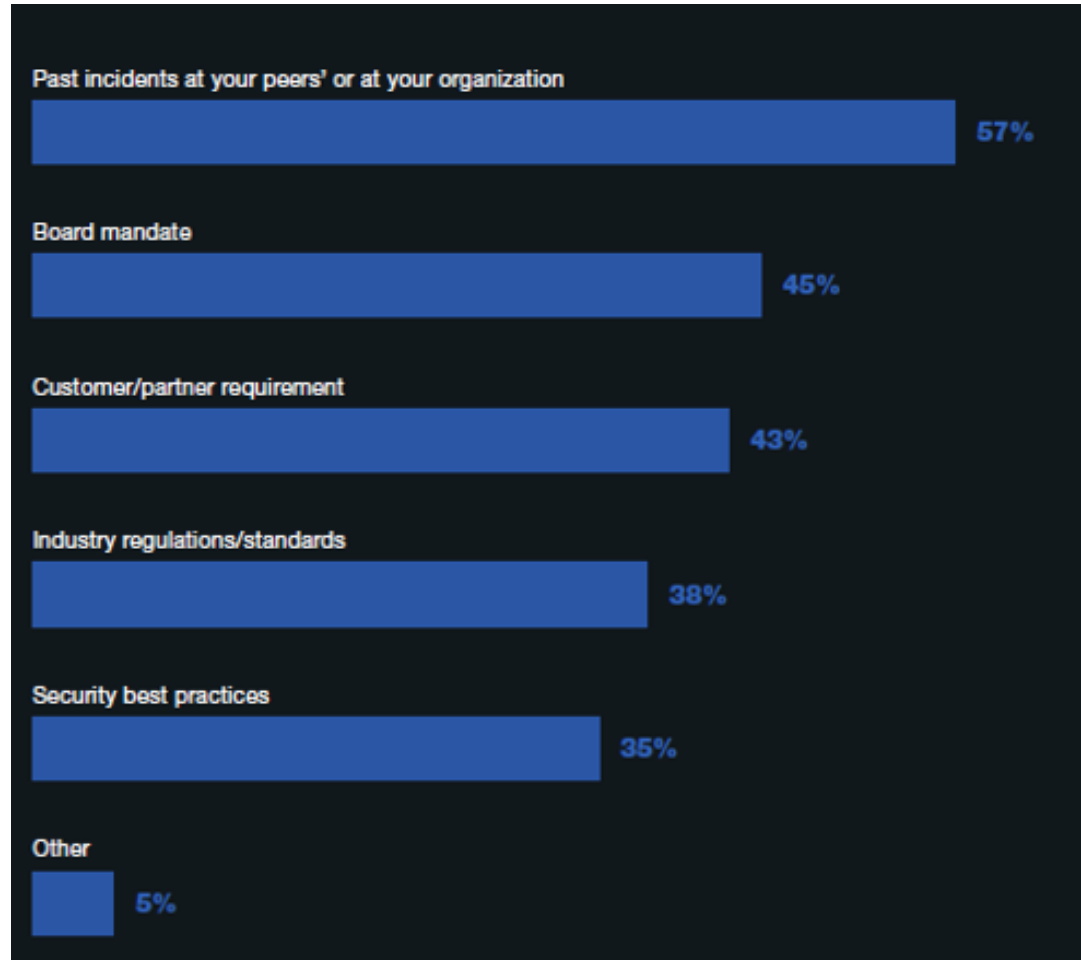
(Purplesec, 2021)



Effects of educational measures

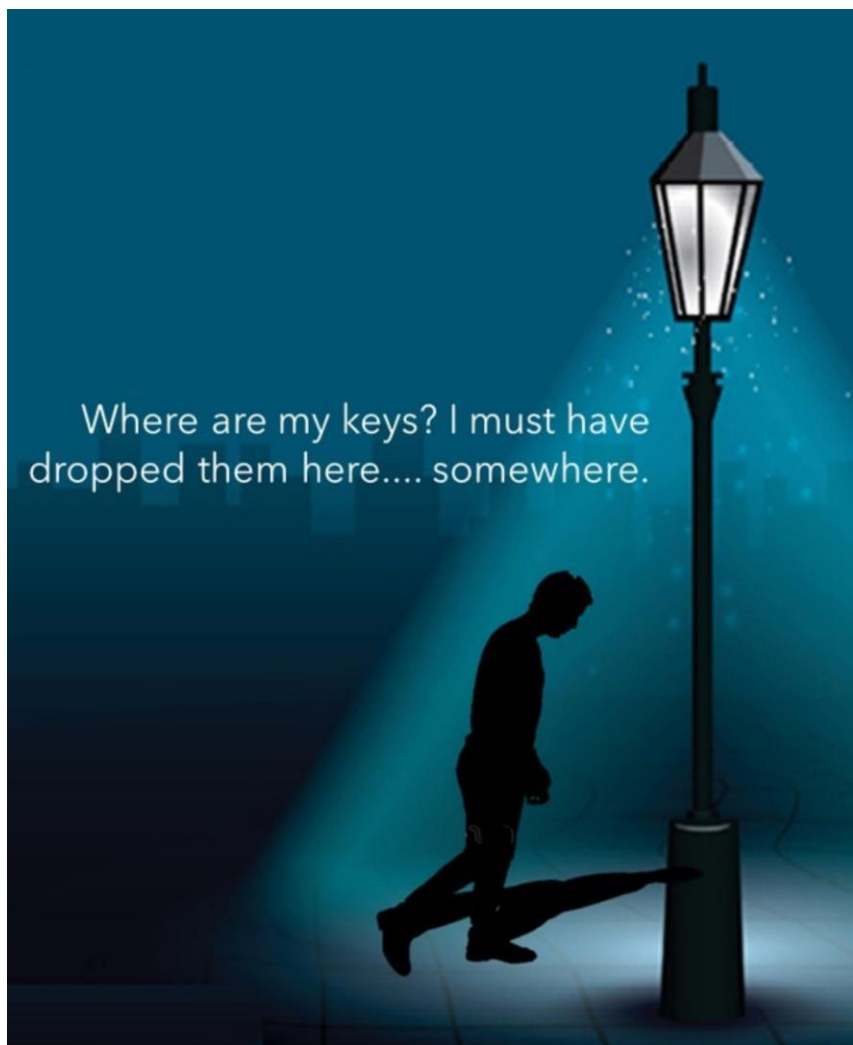
- Good vs. bad IT-Security culture: 5% vs. 1% Susceptibility (KnowBe4, 2022).
 - Information and awareness are not sufficient.
 - Need for progressing into actual intentions, factual behavior and established habits.
- Typical effect size in scientific studies pre/post CS-awareness campaigns: between 20-80% reduction of susceptibility.
 - Enormous potential for improved CS levels.
 - Enormous potential for wasted resources due to ineffective implementation.

Addressing the human factor of CS

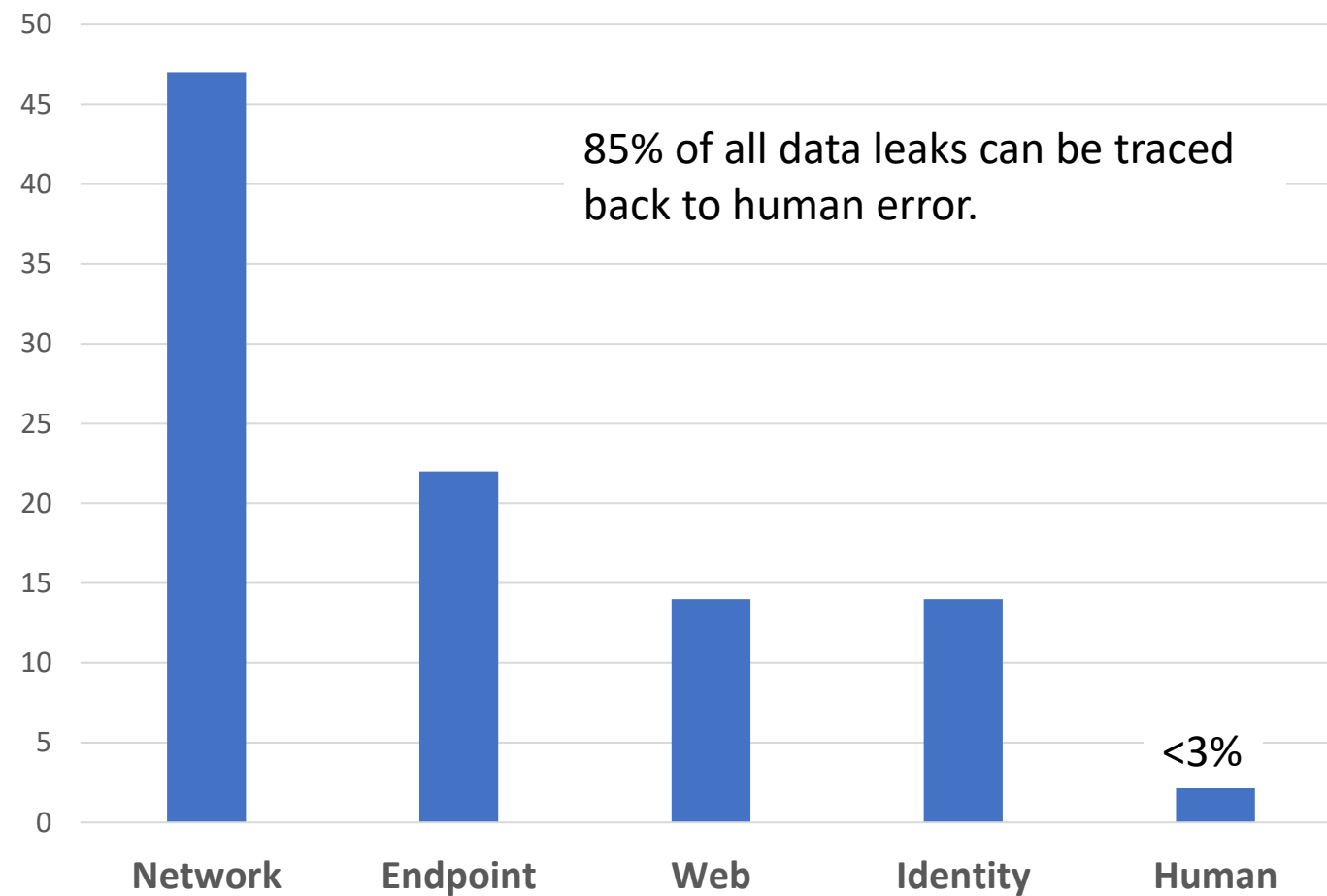


Motivators behind implementation of HF-focused management programs (unintentional insider threats such as e.g. stolen credentials).

(Proofpoint, 2021)



Worldwide IT Security Products Spend - \$BN



(Verizon, 2021)

CYBERSECURITY CURRICULA 2017

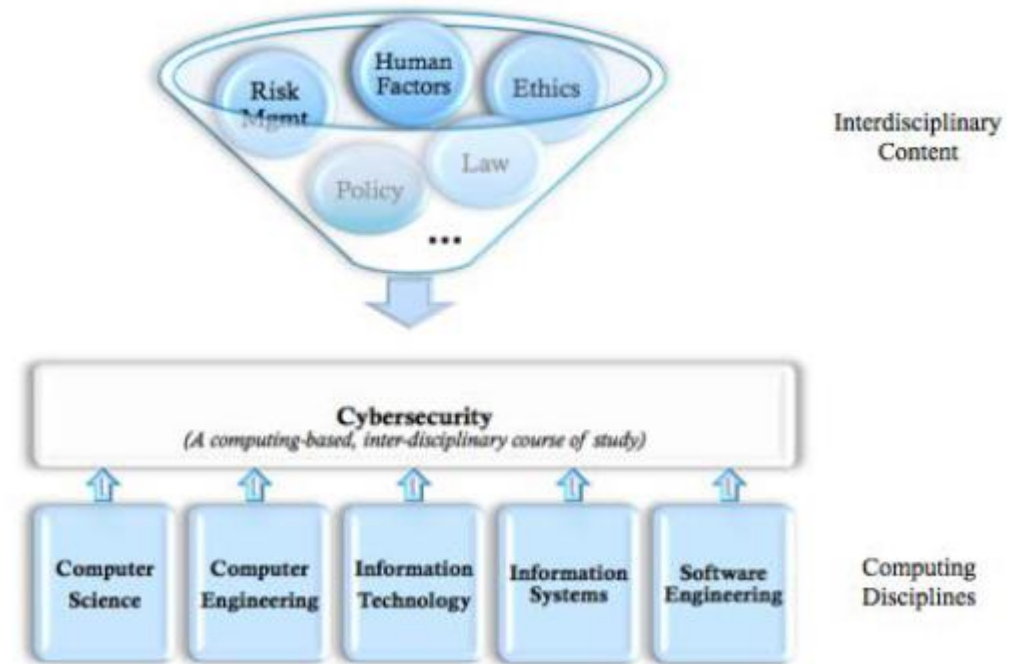
Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series
Joint Task Force on Cybersecurity Education



- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

Version 1.0 Report
31 December 2017



*“A computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, **human factors**, ethics, and risk management.”*

What we offer

- WP IT-Security (tech & human)
- Product-specific risk assessment / Identification of attack vectors and penetration tests (tech & human)
- Consequences for early human-centered design stages (UI) (e.g. usability/security trade-offs)
- Assessment and training of security-relevant human cognition and behavior – identification of educational needs: skills, knowledge, habits
- Simulation and training to enhance CS awareness and actual behavior
- Conceptual work for patient information, consequences for patient-centered care and clinical decision-making

Literature

Baranchuk, A., Refaat, M. M., Patton, K. K., Chung, M. K., Krishnan, K., Kuttyifa, V., ... & American College of Cardiology's Electrophysiology Section Leadership. (2018). Cybersecurity for cardiac implantable electronic devices: What should you know? *Journal of the American College of Cardiology*, 71(11), 1284-1288.

Das, S., Siroky, G. P., Lee, S., Mehta, D., & Suri, R. (2021). Cybersecurity: the need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm*, 18(3), 473-481.

Maisel, W. H., Paulsen, J. E., Hazelett, M. B., & Selzman, K. A. (2018). Striking the right balance when addressing cybersecurity vulnerabilities. *Heart Rhythm*, 15(7), e69-e70.

Siddamsetti, S., Shinn, A., & Gautam, S. (2022). Remote programming of cardiac implantable electronic devices: A novel approach to program cardiac devices for magnetic resonance imaging. *Journal of Cardiovascular Electrophysiology*, 33(5), 1005-1009.

Tomaiko, E., & Zawaneh, M. S. (2021). Cybersecurity threats to cardiac implantable devices: room for improvement. *Current Opinion in Cardiology*, 36(1), 1-4.

Contact

Stefan Sütterlin |

Faculty of Computer Science | Albstadt-Sigmaringen University | Germany

Faculty for Health and Welfare Sciences | Østfold University College | Norway

Centre for Digital Forensics and Cyber Security | Dept. for Software Science | Tallinn University of Technology | Estonia

stefan.suetterlin@hs-albsig.de

stefan.sutterlin@hiof.no

stefan.sutterlin@taltech.ee