WHY HEALTHCARE CYBERSECURITY IS HARD

UNDERSTANDING THE CONSTRAINTS OF HEALTHCARE CYBERSECURITY

There is enormous potential in technology to revolutionize healthcare[1]. Healthcare's connected movement, catalyzed by the HITECH Act of 2009, has connected a previously siloed ecosystem; achieving better clinical outcomes[2], efficiency[3], and cost savings[4]. This simultaneously increased cybersecurity risk[5,6], by incentivizing connectivity without comprehensive security by design[7].

The sobering reality is that all the promise held in technology advancing healthcare is foundationally reliant on security. Unfortunately, not only does the healthcare supply chain inherit what makes information security hard[8], healthcare additionally inherits economic constraints that allow security debt[9] to pass to consumers.

ECONOMIC CONSTRAINTS

Constraint 1: Healthcare optimizes for healthcare

Constraint 2: Security debt accumulates & problems manifest for consumers

Constraint 3: Adversaries exist

Constraint 4: Security requires deep specialization

Constraint 5: US healthcare governance is fragmented

Constraint 6: Uncertainty breaks existing risk models

The extent to which healthcare is able to achieve a sufficient-state of security and resiliency[10] will be proportional to how the healthcare supply chain reduces security debt, not by how well it manages risk.

Figure 1 *Simplified, medical device-specific, healthcare supply chain - Due to economic constraints, security debt (negative externality) is incorporated into healthcare technology by the technology producers which include upstream technology vendors (Tech) as well as healthcare specific stakeholders such as Medical Device Manufacturers (MDM). MDMs assemble final products (medical devices) for consumption by healthcare consumers; Healthcare Delivery Organizations (HDOs), Clinicians, and Patients. Security debt accumulates, adversaries exist, and problems manifest for the consumers. Consumers must consume and manage the risk associated with the accumulated security debt to deliver healthcare.*

[1] FDA Launches the Digital Health Center of Excellence

[2] Transparent sharing of digital health data: A call to action

[3] HITECH reduced the number of manual, paper based record keeping process.

[4] Simple Digital Technologies Can Reduce Health Care Costs

[5] REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

[6] The Evolving State of Medical Device Cybersecurity | Biomedical Instrumentation & Technology

[7] Health Insurance Portability and Accountability Act (HIPAA) incentivizes protections for specific data called Protected Health Information (PHI) and largely penalizes the consumers of healthcare technology, not producers. HITECH did introduce additional security requirements, audits, and fines, but overall these improvements did not offset the increased risk due to the new and interconnected technologies. HHS' "The Security Rule"

[8] Why Information Security is Hard -- An Economic Perspective

[9] Security debt is defined as a type of technical debt; vulnerabilities that come from architecture & design choices, implementation errors, 3rd-party software, configuration, deployment, and maintenance errors.

[10] Executive Order -- Improving Critical Infrastructure Cybersecurity | whitehouse.gov

CONSTRAINT 1:

HEALTHCARE OPTIMIZES FOR HEALTHCARE

Healthcare technology is built by producers such as MDMs and users by consumers; namely HDOs, clinicians, and patients. And these consumers make purchasing decisions based on the ability of those technologies to deliver healthcare features. MDMs, being rational actors, optimize for building healthcare features that support bottom line growth. Not security features which have indirect returns on investment.

Specialization is efficient. If you try to make healthcare experts into security experts you'll get worse healthcare and inadequate security[11]. Healthcare consumers, predominantly HDOs, each year spend between 10 to 20 billion dollars[12] on cybersecurity products, services and fines., This spend is expected to rise[13]. Even with this spend, healthcare performs worse in all key security metrics[14], including spending, detection, and time to resolution.

From a worse healthcare perspective, a 2019 study out of Vanderbilt[15] showed correlation between breaches resulting in worse healthcare outcomes. The controls put in place post-breach hampered the care delivery processes, for example time to administer critical diagnostic tests like an ECG went up by 2.7 minutes, and the 30 day acute myocardial infarction mortality rate increased by 0.36% over a 3 year post breach time period[16].

> “
>
> SPECIALIZATION IS EFFICIENT. IF YOU TRY TO MAKE HEALTHCARE EXPERTS INTO SECURITY EXPERTS YOU'LL GET WORSE HEALTHCARE AND INADEQUATE SECURITY.
>
> ”

CONSTRAINT 2:

SECURITY DEBT ACCUMULATES AND PROBLEMS MANIFEST FOR CONSUMERS

The reasons that attacks are successful reflects, in part, that the ~20 billion dollars invested in healthcare security is largely spent by the consumers of the technology to manage security debt, not reduce debt. Consumers try to manage the security debt by building network and perimeter-based defenses. Three distinct problems arise in the consumer management of security debt.

- The variability of the robustness of this perimeter is high, and therefore devices with security debt are differentially vulnerable depending on what organization bought and deploys them.
- Reliance on perimeter and network defense is necessary but not sufficient.
- Changes in technology and care delivery models are diffusing the traditional security perimeter (e.g., cloud-based services or telehealth).

Healthcare technology consumers have no choice; they must consume that debt to deliver healthcare, otherwise there is no healthcare. Not purchasing a piece of revolutionary medical equipment because it runs on Windows XP[17] is absurd from a clinical perspective, but a sound judgment from a security perspective. When push comes to shove, clinical needs to win.

[11] 2020 Healthcare Data Breach Report: 25% Increase in Breaches in 2020.
[12] The 2020 Healthcare Cybersecurity Report
[13] https://www.globenewswire.com/news-release/2020/09/30/2101131/0/en/Global-Healthcare-Cyber-Security-Market-Is-Expected-to-Reach-USD-33-65-Billion-by-2027-Fior-Markets.html
[14] "2019 Cost of a Data Breach Study," IBM.com 15 Data breach remediation efforts and their implications for hospital quality
[16] The results of the Vanderbuilt study have been critiqued here Cybersecurity implications for hospital quality.
[17] 2020 Unit 42 IoT Threat Report 2020 Unit 42 IoT Threat Report

CONSTRAINT 3:

ADVERSARIES EXIST

Cyber risks are a public health risk and the ever-present reality of cyber-attacks[18,19,20] is an assault to our healthcare delivery supply chain. Attacks across the supply chain not only disrupt the operations of individual hospitals[21] but also impact the entire health systems such as what happened during WannaCry[22], diverting patients contributing to delays in care[23,24] and probably adverse events.[25,26] An example of how devastating a single cyber attack can be is NotPetya which cost Merck and others, individually, hundreds of millions of dollars and disrupted supply chains for drugs and vaccines, and caused collective economic damage around USD 10 billion[27].

The data show attacks on healthcare during the SARS-CoV-2 pandemic and related supply chains increased[28]. HDOs business models were severely impacted such that remaining solvent was a struggle[29], resulting in budgets for IT being cut[30] further reducing the ability of consumers to manage security debt.

CONSTRAINT 4:

SECURITY REQUIRES DEEP SPECIALIZATION

Security is a harsh discipline, it is not kind to amateurs nor professionals. Sub-optimal, but present market forces are slowly shifting the burden of security left in the supply chain to producers. It doesn't solve the problem facing MDMs however. Minimizing the attack surface in products takes a sustained, organization-wide commitment ; a secure development lifecycle and the resources to execute design, implementation, and maintenance, efficiently on a continuous basis, year after year. Because MDMs optimize for healthcare, any spend for security will be unsustainable in existing business models. Meaning the cost to hire expertise, develop foundational infrastructure and individual security features will cost far more than to purchase commercially available solutions.

MDMs traditionally solve problems internally, which makes sense. Microsoft isn't in the pacemaker algorithm business and MDMs do not shy away from tough problems, like keeping failing hearts beating. Healthcare has unique use cases that can make commercial security solutions unusable. Without sufficiently healthcare-specific off-the-shelf solutions, MDMs are forced to "roll their own" solutions, which costs more, are prone to errors, and requires on-going maintenance for the decades long life of products. Commitment for security features that are sub-optimally incentivized by the market, is a tough sell for business leaders within MDMs that are competing on clinical features.

[18] UHS Health System Ransomware Attack, Security Probed by Senator

[19] Vermont governor deploys National Guard in response to UVM cyberattack

[20] Erie County Medical Center confirms ransomware attack led to computer system shutdown

[21] Los Angeles hospital paid $17,000 in bitcoin to ransomware hackers

[22] Investigation WannaCry cyber attack and the NHS (Summary).

[23] A Patient Dies After a Ransomware Attack Hits a Hospital. It was determined in subsequent criminal investigation that the patient would have died regardless and ransomware wasn't the cause of death

[24] Ransomware did not kill a German hospital patient.

[25] Delays in Emergency Care and Mortality during Major US Marathons | NEJM.

[26] A retrospective impact analysis of the WannaCry cyberattack on the NHS This study found that adverse events decreased during the attack but was correlated with decreased admissions.

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

[28] Canalys: More data breaches in 2020 than previous 15 years despite 10% growth in cybersecurity spending

[29] Hospitals and Health Systems Face Unprecedented Financial Pressures Due to COVID-19 | AHA

[30] Hospital Revenue Cycle IT Budgets to Take a Hit After COVID-19

CONSTRAINT 5:

US HEALTHCARE TECHNOLOGY GOVERNANCE IS FRACTURED

Neither electrons nor attackers abide by nearly arbitrary regulatory jurisdictions. Attackers don't care that a piece of technology does or doesn't meet the definition of a medical device[31]. Who regulates the security of healthcare technology that doesn't meet the definition of a medical device, or eletronic health record, or contain protected health information? Are these technologies any less vulnerable? Do they not serve as attack vectors?

At a broader level, the US regulatory oversight of technology with respect to healthcare is fractured (Figure 3). In the absence of a single healthcare technology authority, enhancing healthcare security and resiliency takes a coordinated effort between existing regulators towards creating legal requirements for security by design. Without a coordinated effort, certain healthcare technology verticals will remain large attack surfaces and the interfaces between regulated technologies will continue to experience suboptimal market incentives for reducing security debt.

OVERSIGHT OF THE HEALTHCARE INDUSTRY

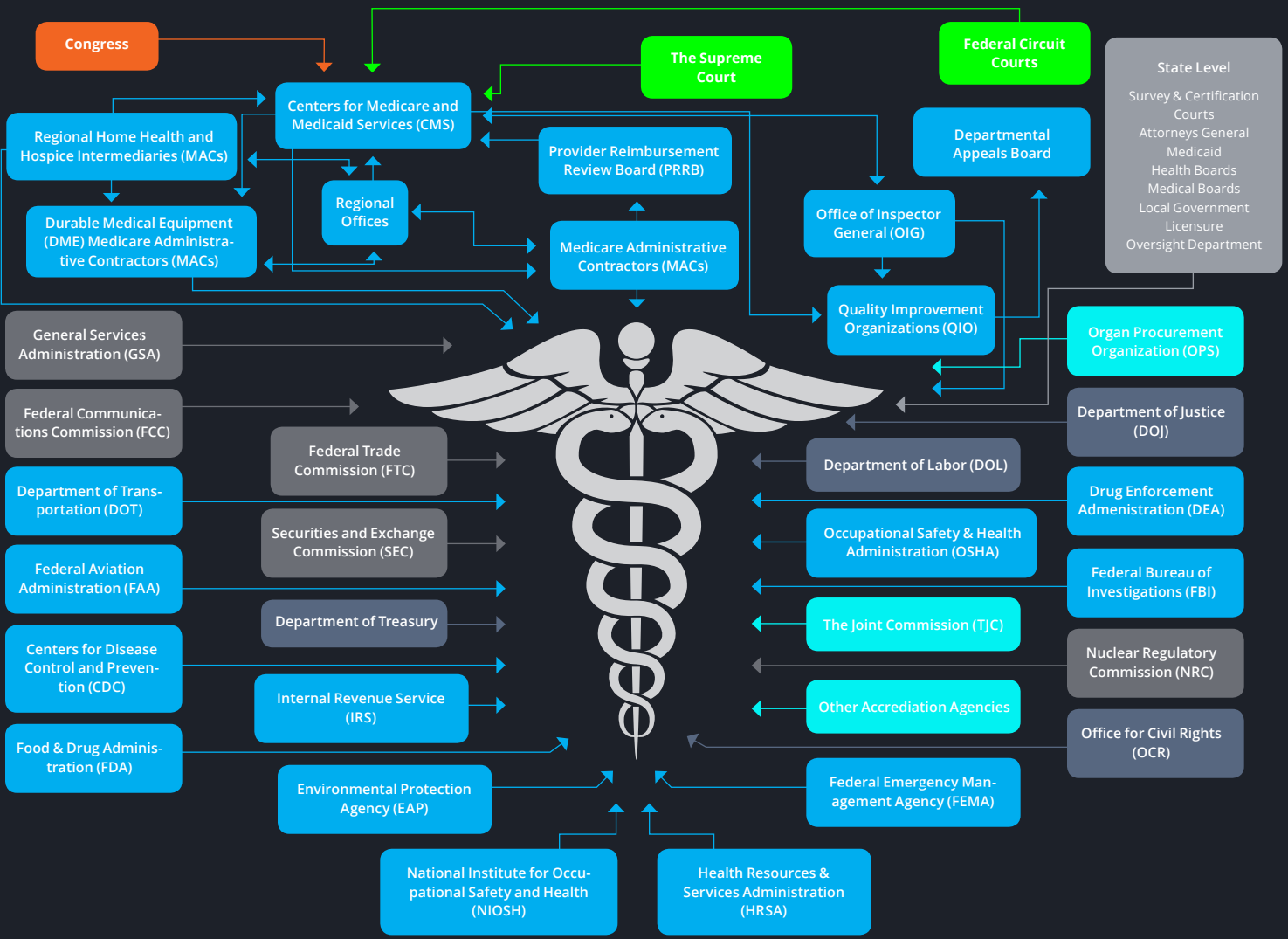

***Figure** 2 Reproduced from the Health Care Industry Cybersecurity Task Force Report, Figure 3, pg 13* REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

[31] A medical device is defined per Section 201(h) of the Food, Drug, and Cosmetic Act. https://www.law.cornell.edu/uscode/text/21/321

CONSTRAINT 6:

UNCERTAINTY BREAKS EXISTING RISK MODELS

The FDA is a market force and serves, in part, to level the playing field of information asymmetry for the consumer. While it makes perfect sense for regulators to step in with respect to cybersecurity, regulators like the FDA are also subject to constraints 1 and 5 above.

Security is continuous and dynamic, but the US FDA regulatory model was built for technology that is static. Specifically with FDA's Center for Devices, Quality System regulations are based on current Good Manufacturing practices (cGMPs) which are a methodology to control for the quality, safety, and efficacy of a deterministic and static system such as a pill. Medical devices and their supporting technologies form systems of systems, which are neither deterministic nor static.

Clinical trials provide a mechanism to assess safety and efficacy of a chemical entity in the human body, but since these chemical entities had to be manufactured at scale, variability or defects in the manufacturing process could introduce uncertainty into the reasonable assurance equation. Therefore, these control mechanisms manifested for drugs as the current Good Manufacturing Practices.[32] Far more uncertainty accompanies the design, manufacture, protection, and maintenance of computing systems, necessitating a fundamental change in the regulatory model, the FDA agrees[33,34,35,36].

While the future of the regulatory model is unclear, it's important to understand the fundamental ways that pills and software differ. At a high level, reducing uncertainty of software-based computing systems of systems during the build and use phases will require a blend of; systems risk management[37,38,] secure systems architecture, and software quality/assurance methodologies, coupled with robust, real-time monitoring of field devices correlated with medical outcomes (Figure 2).

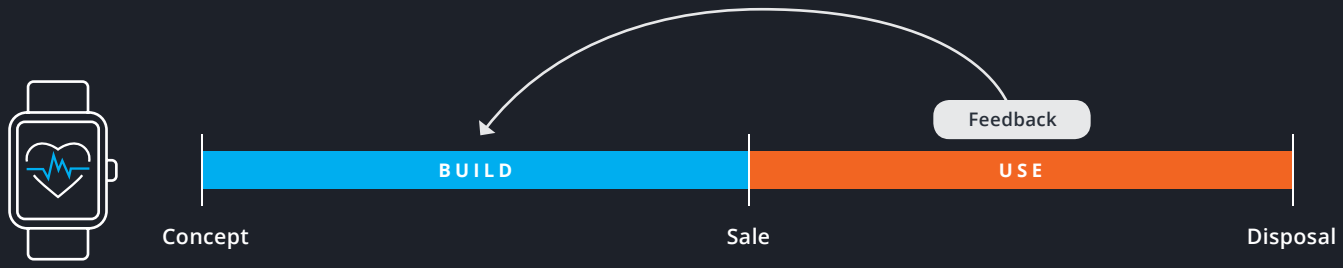

***Figure** 3 The build phase of a pill reduces uncertainty such that drug manufacturers optimize for the time of sale and can rely on slow feedback mechanisms to find problems. Device manufacturers by virtue of copying the pill lifecycle regulatory models, also optimize for sale, but inherit far more uncertainty and will require far more robust and real-time feedback mechanisms to detect postmarket signals and issues.*

[32] Facts About the Current Good Manufacturing Practices (CGMPs)
[33] Jeff Shuren, "We need to rethink the whole thing" https://static1.squarespace.com/static/5a787b5b32601ebcc98b403c/t/5e5ec5b5ef71681f623e8eb8/1583269316110/Shuren+MP+Oct+2019+UL.pdf
[34] Jeff Shuren, "The model isn't fit for purpose" What Policy and Legislative Changes Are Needed to Continue to Digitally Transform Healthcare After COVID-19 2020 Virtual Body Computing Conference
[35] Digital Health Software Precertification (Pre-Cert) Program
[36] It's important to note that FDA's authority and regulatory framework is given by Congress.
[37] (PDF) How complex systems fail
[38] Engineering a Safer World Systems Thinking Applied to Safety

CONCLUSION

By recognizing and calling attention to these fundamental constraints, we can collectively work on solutions that address these root causes and thereby direct limited resources to efforts that will overcome these constraints.

Seth D. Carmody, PhD, seth@medcrypt.co

Disclosures: The authors of this paper are employed by MedCrypt Inc, a medical device cybersecurity software developer.