Stakeholder Dissonance Impedes Medical Device Cyber-Risk Reduction

Elizabeth A. Samaras and George M. Samaras

Elizabeth A. Samaras, *DNP, RN, CPE, HEM, is president-partner of Samaras and Associates, Inc., in Pueblo, CO. Email: libby@samaras-assoc.com*

George M. Samaras, *PhD, DSc, PE, CPE, CQE, CBA, is managing partner of Samaras and Associates, Inc., in Pueblo, CO. Email: george@samaras-assoc.com*

Safety refers to freedom from unintentional harms, and security refers to freedom from intentional harms. Survival compels us to seek out both safety and security. As in the physical world, failure to implement appropriate cybersafety and -security measures can result in physiological, psychological, social, and/or financial harm, with the underlying assets being the natural rights to life, liberty, and property asserted by John Locke.

Risk is characterized as the uncertainty of the deviation from an expected outcome.[1] Cyber risk, therefore, is when we can no longer rely on the cybersecurity outcomes that we have grown to expect. In the healthcare domain, cyber risk is the uncertainty that the interoperating system elements (e.g., users, medical devices, aggregation devices and channels, remote computing systems) possess confidentiality, integrity, and availability (CIA)[2]—the identified triad of information security.

As a top target for cyber assault,[3] the healthcare industry is a new epicenter for malicious cyber threats. Increasingly, risks related to interoperability and usability of interconnected medical devices include cyber risks that threaten both safety and security. Hence, this risky and insecure cyber milieu can, has, and will continue to adversely affect quality, consistency, and availability of care. The impetus for reducing these risks is intensifying and of increasing concern to medical device stakeholders, including agencies at all levels of government and the private sector, manufacturers, and users. However, more must be done.

This commentary provides historical analogies that parallel the current-day cyber-risk environment. It also seeks to critically analyze systemic factors, particularly those among medical device stakeholders that impede or undermine cybersafety and -security. Further, it describes opportunities for cyber-risk mitigations, including the important tasks of recognizing and acting upon stakeholder consonance, as well as identifying and managing stakeholder dissonance (SD) within the complex and interconnected healthcare environment. SD refers to conflicts among the needs, wants, and desires (NWDs) of various stakeholders, as evidenced by errors, workarounds, and threats to patient safety and organizational profitability.[4]

Historical Analogies

Human evolution is fraught with threats to safety and security, and human progress often is measured by the level of sophistication of the tools and technology used to meet these dangers. Science and the applied sciences of medicine and engineering are by nature processes of inquiry, often in a perpetual state of flux and stimulated by real or perceived threats.

Ironically, in their quest for truth over the centuries, practitioners of these disciplines also have been beset by unproven theories, errors, and hubris. One example is found in the protracted pursuit of understanding the source of infectious disease and seeking rational and evidence-based approaches to reduce its spread. The ancient Greeks theorized that “bad air” or “night air,” consisting of various noxious vapors, were the cause of diseases such as plague. Later referred to as “miasma” during the Enlightenment,[5] this unproven theory persisted as the dominant explanation for epidemics for centuries until the influential work by Snow pointed to a contaminated community water source as the cause of London’s 1849 cholera epidemic and the pioneering work of Pasteur and Koch resulted in a broader understanding of Germ Theory in the 1860s and 1870s.[6] Without Snow’s “epidemiology” involving meticulous data collection and analysis, the alleged offender in that deadly outbreak would likely have remained “miasma” for decades. This would have seriously undermined any efforts at effective control or prevention.

Semmelweis also contributed to our understanding of infection control and prevention by demonstrating the importance of effective hand hygiene. Through observation, careful documentation, and validation of his findings, he revealed the direct and causal relationship among cadaverous exposure, poor hand hygiene, and childbed (puerperal) fever. He established that improved hand hygiene could result in dramatic reductions in mortality from this scourge.

Unfortunately, Semmelweis's experience as a sentinel offers an extreme kind of object lesson. He was scorned by colleagues, who resented his affront to accepted medical practices, and died precipitously in a mental institution.[7] In Semmelweis's cautionary tale, two major stakeholder groups included the physicians of his day and the perinatal patients under their care. One of these, the other physicians, exhibited an unwarranted degree of professional puffery by aligning themselves with the status quo of current medical practice instead of the needs of patients. This can be viewed as an extreme case of SD with the other major stakeholders of the story: the women who became septic and died.

History is replete with similar cases of egregious professional arrogance and SD. A more recent example can be found when the interests of Tuskegee researchers conflicted with those of "their subjects" with untreated syphilis. More subtle examples of SD also abound, such as evidence that specialists with financial interests in on-site laboratories order more lab tests than their nonowner specialist or primary care counterparts (even when patient and practice characteristics are considered), potentially resulting in millions of dollars in excess healthcare spending.[8]

Parallels with Today

The historical analogies described above have much to offer as we consider our present situation with respect to cyber risk. During the previous half century, medical devices underwent extraordinary evolutionary change, especially in connectivity, rapidly exceeding the abilities of their stakeholders to ensure interoperable safety, security, and usability.[9] Despite rapid increases in the rate of information generation and exchange, we often find ourselves in a cloud of misconceptions, misdirection, or misplaced priorities. This modern-day "cyber miasma" thwarts efforts at reducing cyber risks.

Profound technical gaps in both training and understanding on the part of many stakeholders, and the interoperable medical devices they use, manifest in 1) near magical thinking (e.g., sentiments such as "only authorized persons have access to the monitoring data from my implanted medical device," "they seek only to help me," and "it can't happen to us") and 2) ritualistic behavior (e.g., "if the device connects, is compatible with my port and works, it must be safe and secure" and "we have always disposed of or revamped outmoded equipment this way").

These behaviors or ways of thinking can be especially pronounced among what we term "legacy users"—those healthcare providers (HCPs) and healthcare delivery organization (HDO) managers that were not immersed in the digitalized world early and often. Although resources are available to deal with the cyber risks of today, they are often conflicting, and few have been validated or are evidence based. In our view, knowledge of best practices to reduce medical device cyber risk is in its nascent stages, as shown by repeated and successful attacks. This may be due, in part, because preventive resources are continually challenged and stressed by the mercurial nature of cyber onslaughts that adapt and develop resistance much like their microorganism counterparts in the physical world. However, we assert that widespread failures to appreciate the problem as described earlier (e.g., magical thinking, ritual behaviors and miasma-like levels of understanding, legacy-users, etc.) are important contributing factors.

Despite rapid increases in the rate of information generation and exchange, we often find ourselves in a cloud of misconceptions, misdirection, or misplaced priorities. This modern-day "cyber miasma" thwarts efforts at reducing cyber risks.

Former "sacred cows" of presumed protection are now being debunked after decades of practice. For example, according to McMillan, "The man who wrote the book on password management has a confession to make: he blew it."[10] According to National Institute of Standards and Technology guidelines, creating complex passwords and updating them frequently does little to safeguard security; instead, this practice has "a negative impact on usability."[10]

These supposed safeguards, which were not evidence based to begin with (i.e., never validated), instead resulted in decreased productivity and increased cyber risk and rates of human error. Like the early pushback Semmelweis encountered from an uninformed and entrenched status quo, it will likely take time to dispel old cybersecurity conventions that offer misplaced perceptions of cyber-risk reduction in lieu of properly vetted approaches to cyber hygiene.

Stakeholders, their NWDs, and SD

Stakeholders are both individuals and groups of individuals (formal or informal) who can affect or be affected by the decisions, actions, policies, and procedures regarding a project, process, or product. Understanding the roles played by various stakeholders and recognizing SD are important and underappreciated factors in addressing the problems of medical device cyber risk. We assert that analyzing the NWDs of various medical device stakeholders and identifying where these NWDs diverge (i.e., SD) will provide unique insights for cybersecurity and targeted opportunities for cyber-risk management.

Analyzing the NWDs of various medical device stakeholders and identifying where these NWDs diverge (i.e., SD) will provide unique insights for cybersecurity and targeted opportunities for cyber-risk management.

The following is an overview of the process for undergoing this type of analysis. Relevant examples also are provided to make the case for more formal SD analysis as an important strategy for cyber-risk reduction.

Step 1: Identify the Stakeholders

Ideally, as a first step, one would identify the full universe of entities with a stake in medical device cybersecurity. Although such a process is beyond the scope of this commentary, we can nevertheless begin by identifying several high-level stakeholder categories by following a medical device from conceptualization through use (but not disposal). They include manufacturers, HDOs, HCPs, patients and lay caregivers, regulators, and third-party payers.

Step 2: Identify the NWDs of Stakeholders

Providing a comprehensive analysis of NWDs is beyond the scope of this article. Debates over the differences among needs (must have), wants (want to have), and desires (I'll know it when I see it) will always persist. These distinctions are not central to this discussion; therefore, we have collapsed all examples into NWDs. The following are examples of relevant NWDs for various cybersecurity stakeholders in healthcare:

Manufacturers. A pathway to market (preferably rapid) for their products; reimbursement authorization by third-party payers; robust sales of devices and consumables to HDOs, patients, and lay caregivers; protection for their proprietary intellectual property; less regulation and less competition; and safety and effectiveness.

HDOs. Devices that are safe and effective to use and that engender user satisfaction; appropriate and secure interfacing with existing systems; robust reimbursement; cyber-risk transparency and implementation simplicity provided by manufacturers; comparable or lower costs and complexity (given the nature of the devices).

HCPs. Devices that are easy to learn and use and that do not (or only minimally) disrupt workflow; devices that are acceptable to patients; devices that have the potential to optimize time and care quality in an efficient and potentially financially beneficial manner.

Patients and lay caregivers. Devices that are safe, effective, secure, and easy to use; devices that are available at no or low out-of-pocket cost.

Regulators. Devices that are safe, effective, and secure; cooperation, transparency, and compliance from the regulated communities.

Third-party payers. Proven, cost-effective devices and quality systems with demonstrable diagnostic/therapeutic contributions consistent with standard of care or improved outcomes; efficient documentation and accountability metrics.

Step 3: Recognize Consonance among Stakeholders

Several areas of agreement, in principle, can be seen among stakeholders. Examples of general stakeholder consonance gleaned from the examples above include devices that are safe, secure, effective, and easy to use; have acceptable life cycle costs, including for purchase and use; and give a diagnostic or therapeutic edge or are more efficient.

Step 4: Identify SD

This is a critical step in the process and a major focus of the current work. As such, it will be discussed in detail in the following sections.

Sources of SD

SD within a Category: Regulatory

Stakeholders are rarely monolithic; typically, they are diverse even within their category or class. For example, a variety of regulatory entities attempt to influence the cybersecurity-related behaviors of system stakeholders in the United States. As a result, discrepancies and conflicts exist both within and among regulatory entities. Regulators include federal and state agencies and nongovernmental organizations (e.g., The Joint Commission), nationally recognized testing laboratories, and others. At the federal level, their activities include:

- Regulation of the marketing of medical devices (Department of Health & Human Services [HHS]/Food and Drug Administration/Centers for Devices and Radiological Health [CDRH])
- Adoption and promotion of health information exchanges (HHS/Office of the National Coordinator for Health Information Technology [ONC]).
- Protection of health information privacy rights (HHS/Office for Civil Rights [OCR]).
- Protection from health, safety, and security threats (Department of Homeland Security [DHS] and HHS/Centers for Disease Control and Prevention).
- Protection of critical national infrastructure, such as the healthcare system, which in turn depends on other critical infrastructure, including power, water, and waste (various elements of DHS).
- Partnerships with state and territorial agencies to enforce many healthcare regulations (HHS/Centers for Medicare & Medicaid Services [CMS]), especially through CMS's activities as a third-party payer.

We believe that proper communication and coordination regarding effective cyber-risk mitigation are lacking within and among the regulatory entities noted above. Examples of SD among these regulators and their ramifications include:

- ONC's push for interoperability without ensuring/enforcing concomitant cybersecurity. (Interoperability/connectivity is a fundamental driver for cyber risk.)
- OCR's emphasis on health information privacy without clear or consistent recognition/enforcement of all aspects of cyber-risk control. (For example, unintended breach of 500 patient records is bad [and reportable], but when only 499 records are involved, it's okay [and not-reportable].)[11,12]
- CDRH claims risk-based decision making and offers expectations for—but eschews rigorous regulation of—medical device cybersecurity.[13–15] The agency's historically weak pre- and postmarket regulation of software, even in high-risk medical devices, does not enforce a "cybersecure by design" paradigm; therefore, the most basic healthcare infrastructure cyber-risk problems are not addressed.

An additional related source of SD includes efforts by various stakeholders to limit, or even eliminate, rigorous software regulation of certain types of healthcare technology, such as pushback against regulation of electronic health records (EHRs) as medical devices.[16] This may have seemed appealing in the short term; however, in the long term, we expect that it will undermine everyone's performance and financial bottom line, as flawed software is fundamental to failures in connectivity, interoperability, and cybersecurity in an increasingly software-dependent healthcare environment.

SD among Categories: Privacy

Just as any given stakeholder class is rarely homogenous, different categories of stakeholders rarely share a wholly common understanding of relevant concepts and constructs. One example is privacy, which can be defined as "freedom from unauthorized intrusion."[17] If privacy is violated, reputational, financial, psychological, or even physical harms can result. The need to provide appropriate "authorized access" is an important corollary to privacy. In addition to threatening the individuals and organizations involved, unauthorized access or breaches of privacy carry the likelihood of downstream and broader impacts.

Considering medical device cyber risk, it is apparent that most, if not all, stakeholders have a vested interest in their interpretation of privacy protections, as these are considered central to current societal notions of security and stability in the United States. However, when we begin to parse out the concept of privacy and related constructs (e.g., confidentiality, secrecy, ownership), consonance begins to fade among stakeholder groups and underlying, and oftentimes profound, SD emerges. Here are a few examples:

- Patients and their authorized designees have legal rights to privacy and access to their protected health information under the Health Insurance Portability and Accountability Act (HIPAA). Despite these rights, access does not currently extend to data collected on patients via implanted medical devices such as implantable cardiac defibrillators. Instead, patient data are transmitted, controlled, and essentially "owned" by manufacturers and delivered to HCPs for "translation" to patients. Regulatory considerations, liability issues, and concerns regarding patients' ability to interpret these data have been argued in defense of this exception.[18] Nevertheless, this practice threatens key components of the CIA triad, affecting the availability and integrity of information. When these principles are violated, patients and lay caregivers are potentially left without real-time access to or credible assurances of the completeness of information. This could result in failures to forewarn them of a malfunction, cyber breach, or ominous status change.
- HDOs and HCPs are bound by rigorous HIPAA guidelines attendant upon safeguarding the privacy of individuals' protected health information and stringent associated penalties for breaches. Forums and conferences exist for discussing responses to or ameliorating these problems after the fact. However, the simultaneous threat of penalty (and reputational damage) oftentimes fosters less-than-transparent communication regarding breaches, resulting in failure to share timely information with other stakeholders, impeding cyber-risk reduction.
- Manufacturers invest heavily in development/commercialization and are justifiably sensitive to the release of proprietary information, especially to competitors. They can be hesitant to undermine their market position with public reporting of problems.[19] Even in the presence of legitimate business reasons, manufacturer failures of transparency or delays in notification of problems can cause substantial SD. Such failures can hinder HDOs, HCPs, regulators, or other stakeholder efforts to mitigate cyber risk as a public health imperative.

When we begin to parse out the concept of privacy and related constructs (e.g., confidentiality, secrecy, ownership), consonance begins to fade among stakeholder groups and underlying, and oftentimes profound, SD emerges.

These basic examples of SD undermine the notion that privacy is a shared conceptualization—or even a shared value—among disparate stakeholder categories or classes. These differences of interpretation can be viewed largely as a function of divergent self-interests among these stakeholders, which can readily result in behaviors that impede progress in preventing, identifying, or correcting cyber risks.

Other Relevant Examples

From a human-centered systems complexity model perspective,[20] we can recognize complexity and human error at various levels that present cyber risks for medical devices and healthcare in general. We can also readily observe failures at multiple levels of system complexity, from micro to mega, such as managing cybersecurity credentials (micro-ergonomic), cybersecurity fatigue (meso-ergonomic), cyber-risk ownership rejection (macro-ergonomic), and cyber myopia—the failure of various subcultures to fully appreciate the breadth and depth of cyber risks (mega-ergonomic). Recognized problems are listed in Table 1, which has been organized according to this complexity model. In our opinion, the problems shown in Table 1 have some element of, or can be traced to, conflicts among the NWDs of two or more stakeholders (i.e., traced to SD). In addition to recognized cybersecurity problems, the table also includes examples of the stakeholders involved and likely sources of SD. By organizing it this way, one can begin to consider effective interventions at each level.

Resolution of SD

After stakeholders have been identified and their NWDs and areas of SD discerned, the challenge of managing SD can be considered.

System stakeholders (e.g., manufacturers, HDOs, HCPs, lay caregivers and patients) arguably have a primary motivation (e.g., safe and effective care) but little capability to influence each other's behavior with respect to cyber-risk reduction. Conversely, stakeholders such as regulators and third-party payers arguably have the primary capability (e.g., via strategies such as the denials of device clearances or reimbursements, respectively) to compel more effective cybersecurity solutions for medical devices and their use. However, in the absence of full appreciation of the complex and varied problem-etiology-solution dynamics, these players may have limited motivation and few direct mechanisms to influence stakeholder behavior toward effective safeguards.

Uncovering SD at each level of the system, including ways that stakeholders' self-interest and opportunities for proactive intervention overlap or diverge, will expose problem etiology and may offer viable solution options. Of necessity, management of SD will be an iterative process that requires continual reengagement in the presence of dynamic changes.

Discussion and Recommendations

No single category of stakeholders will have complete information, understanding, tools, processes, standards, and regulations to "identify, protect, detect, respond, and restore"[23] in the presence of escalating incidence of cyberattacks and the resulting increased uncertainty associated with cyber risks.

Complexity Level	Problem Category*	Stakeholders	Stakeholder Dissonance†
Micro-ergonomics (physical ergonomics)	1) Difficulties managing security credentials (e.g., USB sticks, two-factor authentications, biometrics, bio-embedded chips). 2) Visual information "chameleon" presentation (deceptive look and feel of delivery vehicle [e.g., for phishing]).	1) HDO staff (IT), HCPs, other users. 2) Patients and lay caregivers. 3) Malicious hackers.	1) Nonintuitive solutions. 2) Security practices perceived as cumbersome or inconsistent with workflow.
Meso-ergonomics (information management ergonomics)	1) Cyber fatigue and habituation. 2) Accidental coding errors resulting in vulnerable code.[21] 3) Password management. 4) Legacy devices, legacy software. 5) Nonvalidated interoperability or other control failures. 6) Incomplete or poor encryption practices.[21] 7) Inadequate built-in security protocols. 8) Weak or nonexistent vulnerability reporting.[22]	1) Manufacturers. 2) HDO staff (including managers, IT).	Competing resource allocations within and among enterprises.
Macro-ergonomics (social ergonomics)	1) Agnostic ownership of cyber risks (including ambiguity or rejection of "ownership" responsibility). 2) Legacy providers, legacy managers, and legacy organizations. 3) "Safety culture" or culture of vigilance (e.g., high-reliability organizations vs. "rush to release"[21]; security policies inconsistently employed).[22] 4) Operational/organizational (e.g., siloes within and among stakeholders). 5) Training underprioritized.[22] 6) Failure to change practices postbreach.[22] 7) Norms and roles (discrepancies among IT, HCPs, manufacturers, HDOs, and users). 8) Use of basic technologies only.[22] 9) Widely accepted prevention practices overlooked.[22] 10) Growing detection, response, and resolution times.[22]	1) Manufacturers. 2) HDOs (C-suite and throughout). 3) HCPs.	1) Competing resource allocations within and among enterprises. 2) Unclear or inadequate mission. 3) Unclear delineation of duties among internal stakeholders.
Mega-ergonomics (cultural ergonomics)	1) Cyber myopia (not understanding breaches or the breadth and depth of the problem). 2) Reactive culture (security budgets increase only in response to a hacking incident, rather than using proactive approach.[21] 3) Omissions/failures in public regulation and professional education.	1) Manufacturers. 2) HDOs (managers, IT, "legacy users"). 3) Regulators.	1) Language, training, and cultural differences within and among disciplines. 2) Competing pressures from the regulated community.

Table 1. Stakeholders and stakeholder dissonance: complexity level and associated problems. *Some problems may extend beyond more than one identified complexity level. †Examples for illustrative purposes only. Abbreviations used: HCP, healthcare provider; HDO, healthcare delivery organization; IT, information technology; USB, Universal Serial Bus.

We contend that medical device cyber risk is a joint function of medical device interoperability and usability, in the presence of multiple stakeholders, resulting in a high-complexity problem. Successful interventions must be a joint function of technology and application of human factors knowledge. Purely technological solutions, bereft of human factors knowledge, cannot eliminate human error. Failures of inadequate design controls (including lack of evidence-based validations) and risk management (including the associated lack of transparency of known and foreseeable hazards) transfers the cost of cyber risk from manufacturers to HDOs. HDOs also have their share of responsibility; inadequate or overly burdensome cybersecurity of both legacy and modern medical devices by HDOs transfers cyber-risk costs to HCPs, patients, lay caregivers, and ultimately, to third-party payers and society. However, it is important to keep in mind that unlike the transfer of financial risk, cyber risk related to quality of care (harm to patients, providers, and organizations) is not transferrable. Therefore, it is vitally important to address SD at every level and by all stakeholders.

Purely technological solutions, bereft of human factors knowledge, cannot eliminate human error.

Moving forward, we must rigorously implement identified technical best practices and regulatory solutions, which include:

- Reducing the potential spatial (e.g., fewer ports and fewer connected devices) and temporal (e.g., less "on" or connected time) "attack surface,"[24] rather than continually expanding it, to 1) limit attacks through points of vulnerability and 2) increase the physical and logical separation between safety-critical and non–safety-critical components.
- Conducting comprehensive and transparent risk assessments during development and deployment, as well as iteratively thereafter, to fully appreciate the risks and benefits of devices as conceived, marketed, and used. As a matter of priority, these types of analyses must always recognize that, according to Beau Woods (as quoted by Kuckler), "data are replaceable. Life is irreplaceable."[25]
- Enforcing evidence-based premarket and predeployment validations,[20] as well as transparent hazard analyses and risk controls of all components (including all software components), of connected medical devices and of the entire interoperable system(s) in which they will, or may conceivably, function.[9]
- Engaging in prepurchase vulnerability assessments[26,27] with a designated minimum Safety Integrity Level analogous to that found in the automotive, aviation, and other industrial sectors.
- Enforcing effective public reporting, active surveillance, and rapid response in a manner that does not permit "gaming" (by any of the stakeholders) of the reporting systems intended to protect public health and welfare.
- Adopting high-reliability organization[28] standards of rigor regarding cyber-risk mitigation and a culture-of-safety approach among medical device stakeholder organizations. This includes remaining vigilant from design through disposal with evidence-based approaches to cyber hygiene, which is not a one-and-done proposition but an ongoing public health imperative.
- Targeting and validating interventions/evidence-based approaches at all levels of complexity (for problems of the sort identified in Table 1 and not addressed in this list); retest/reevaluate in the dynamic cyber-risk environment.
- Considering participation in the "bug-bounty" trend. Malicious hackers are hard at work providing a valuable vulnerability assessment service that is neither optional nor free. Engaging ethical hackers can help expose medical device vulnerabilities, which then can be reported to the manufacturer and/or deployer for correction prior to market exposure or incurring postmarket costs.

The healthcare technology community cannot continue to counter real, and potentially lethal, cyber risks with naïve, nonvalidated, or outmoded strategies, incomplete worldviews, inadequate prophylaxis, or magical thinking reminiscent of the era of "miasma as explanation." We must use validated best practices—coordinated, proactive, iterative, and evidence-based approaches—that include rigorous examination of root causes and global reporting/

sharing of lessons learned from previous attacks on medical devices and other systems. Technical methods, such as using secure multiparty computations[9] and shared "ledgers" (blockchain methods), are worthy of consideration. Furthermore, recognizing that cyber-risk reduction will involve more than technological fixes is imperative. As asserted by cybersecurity expert Kevin Fu, this is "a people problem" wherein "the hard part mind you, is the culture."[29] A necessary, but not sufficient, mitigation will involve transparent and collaborative risk management at all levels[9,30] with cooperation and coordination by all stakeholders.

This commentary makes the case for the importance of proactive SD recognition and amelioration as an essential tool for reducing cyber risk. Reactive methods using data analytics and machine learning may be necessary but are likely not sufficient. Finally, it is worthwhile to keep in mind two fundamental, yet relevant, existential perspectives of key stakeholders. The first is that enterprise stakeholders do not exist to be secure (neither in the tangible nor cyber realm). Their fundamental short-term objective is to be financially sustainable, without which they cannot survive. However, this is a source of an inherent and internal SD for them insofar as if they are not secure, increasingly they risk long-term financial stability. The second is that patients inevitably have the most assets at stake (life, liberty, and property) in the presence of unmitigated cyber or real-world risks imposed by the healthcare environment. The latter must always drive our efforts at prevention.

References

1. Samaras GM. Medical Device Life Cycle Risk Management. Available at: www.samaras-assoc.com/PublicDocs/ASQ_BioFeedback_2015.pdf. Accessed May 22, 2018.

2. National Institute of Standards and Technology. Underlying Technical Models for Information Technology Security. Available at: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf. Accessed Aug. 14, 2017.

3. IBM X-Force Research. Reviewing a year of serious data breaches, major attacks and new vulnerabilities. Available at: www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=SEW03133USEN&attachment=SEW03133USEN.PDF . Accessed Sept. 20, 2017.

4. Samaras EA, Samaras GM. Using Human-Centered Systems Engineering to Reduce Nurse Stakeholder Dissonance. *Biomed Instrum Technol.* 2010;44(suppl 1):25–32.

5. Sterner CS. A Brief History of Miasmic Theory. Available at: www.carlsterner.com/research/2007_a_brief_history_of_miasmic_theory.shtml. Accessed Aug. 15, 2017.

6. Harvard University Library. Germ Theory. Available at: http://ocp.hul.harvard.edu/contagion/germtheory.html. Accessed Aug. 15, 2017.

7. Semmelweis Society International. Dr. Semmelweis' Biography. Available at: http://semmelweis.org/about/dr-semmelweis-biography. Accessed Aug. 15, 2017.

8. Bishop TF, Federman AD, Ross JS. Laboratory test ordering at physician offices with and without on-site laboratories. *J Gen Intern Med.* 2010. 25(10):1057–63.

9. Samaras EA, Samaras GM. Confronting systemic challenges in interoperable medical device safety, security & usability. *J Biomed Inform.* 2016;63:226–34.

10. McMillan R. The Man Who Wrote Those Password Rules Has a New Tip: N3v$r M1^d!. Available at www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118. Accessed Aug. 15, 2017.

11. Department of Health & Human Services. Breach Notification Rule. Available at: www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Accessed Aug. 15, 2017.

12. Department of Health & Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed Aug. 15, 2017.

13. Food and Drug Administration. Content of Premarket Submissions for Management of Cyberse-

The healthcare technology community cannot continue to counter real, and potentially lethal, cyber risks with naïve, nonvalidated, or outmoded strategies, incomplete worldviews, inadequate prophylaxis, or magical thinking reminiscent of the era of "miasma as explanation."

curity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf. Accessed Aug. 15, 2017.

14. Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. Available at: www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf. Accessed Aug. 15, 2017.

15. Scott J, Spaniel D. Assessing the FDA's Cybersecurity Guidelines for Medical Device Manufacturers. Why Subtle 'Suggestions' May Not Be Enough. Available at: http://icitech.org/wp-content/uploads/2016/02/ICIT-Blog-FDA-Cyber-Security-Guidelines2.pdf Accessed Aug. 24, 2017.

16. Sullivan T. FDA and Electronic Health Records. Available at: www.policymed.com/2011/08/fda-and-electronic-health-records.html. Accessed Aug. 15, 2017.

17. Merriam-Webster. Definition of "privacy." Available at: www.merriam-webster.com/dictionary/privacy. Accessed Aug. 15, 2017.

18. Campos H. The heart of the matter. Available at: www.slate.com/articles/technology/future_tense/2015/03/patients_should_be_allowed_to_access_data_generated_by_implanted_devices.html. Accessed Aug. 15, 2017.

19. Berkot B. St. Jude halts pacemaker implants due to data, battery issues. Available at: www.reuters.com/article/us-st-jude-medical-pacemaker/st-jude-halts-pacemaker-implants-due-to-data-battery-issues-idUSKCN12S24J. Accessed Sept. 20, 2017.

20. Samaras GM. Reducing latent errors, drift errors, and stakeholder dissonance. Available at: http://content.iospress.com/articles/work/wor0413. Accessed Aug. 30, 2017.

21. Ponemon Institute. Medical Device Security: An Industry Under Attack and Unprepared to Defend. Available at: www.synopsys.com/content/dam/synopsys/sig-assets/reports/medical-device-security-ponemon-synopsys.pdf. Accessed Aug. 24, 2017.

22. SolarWinds MSP. Cybersecurity: Could Overconfidence Lead to an Extinction Event? Available at: www.solarwindsmsp.com/resources/WP-cybersecurity-could-overconfidence-lead-extinction-event. Accessed Aug. 24, 2017

23. National Institute of Standards and Technology. *The Cyber Security Framework: Implementation Guidance for Federal Agencies*. NISTIR 8170 (Draft). Gaithersburg, MD: Department of Commerce; 2017.

24. Fortney C. Should Every Device Be Connected? Weighing the Risks and Benefits of Medical Device Connectivity. Available at: www.meddeviceonline.com/doc/should-every-device-be-connected-0001 Accessed Sept. 13, 2017.

25. Kuckler H. Medical device makers wake up to cyber-security threat. Available at: www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691. Accessed Aug. 15, 2017.

26. Medical Device Innovation, Safety & Security Consortium. MDISS Launches 'WHISTL" Network of Security Testing Labs for Medical Devices. Available at: www.mdiss.org/news/mdiss-launches-whistl-network-of-security-testing-labs-for-medical-devices. Accessed May 22, 2018.

27. Snell E. Medical Device Security Rarely Tested in Healthcare Orgs. Available at: https://healthitsecurity.com/news/medical-device-security-rarely-tested-in-healthcare-orgs . Accessed Aug. 17, 2017.

28. Agency for Healthcare Research and Quality. High Reliability. Available at: https://psnet.ahrq.gov/primers/primer/31/high-reliability. Accessed Aug. 15, 2017.

29. Lee K. Medical device safety needs to be given more attention, an expert says. Available at: http://searchhealthit.techtarget.com/feature/Medical-device-safety-needs-to-be-given-more-attention-an-expert-says. Accessed Aug. 15, 2017.

30. Pavlovic Y, Shilpa P. Filling in the Gaps on Medical Device Cybersecurity. Available at: https://f.datasrvr.com/fr1/017/42746/2017_06_06_Medical_Device_Alert_-_Filling_in_the_Gaps_on_Medical_Device_Cybersecurity_Ver_4.pdf. Accessed Aug. 15, 2017.