FEATURE

Healthcare Security—Three Paradoxes and the Need for a Paradigm Shift

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2GE0yJe

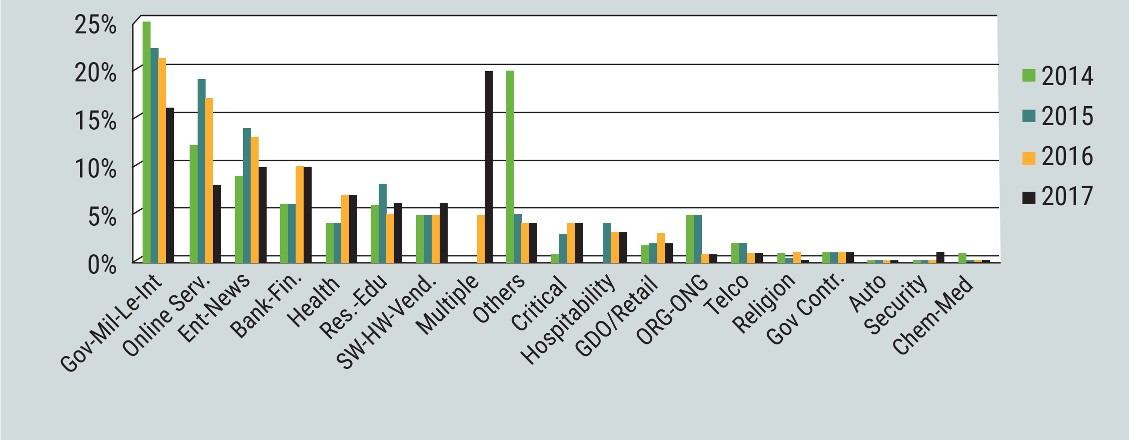
Giuliano Pozza, CGEIT, e-CF Plus (CIO), ITIL v3
Is a biomedical engineer by training and the chief information officer (CIO) of Ospedale San Raffaele, the most important private clinical and research institution in Italy. He is also the president of the Italian Association of Healthcare Information System Professionals. Previously, he was the CIO of Fondazione Don Carlo Gnocchi Onlus, a statewide Italian social care and rehabilitation organization. He also worked for Istituto Clinico Humanitas and in the healthcare practice of consulting firm Accenture.

Is the chief information officer (CIO) role still relevant for IT security in healthcare? The world of information and data management is changing faster than anyone could have predicted a few years ago, and attention to sensitive data protection is growing, as the new European Union General Data Protection Regulation (GDPR) is clearly proving. The role of the CIO as the custodian of information and data, in healthcare or other contexts, is increasingly becoming paradoxical in many ways.[1] One of the crucial pain points of healthcare CIOs is definitely security, albeit IT security is not in any way a neglected item in CIOs' agendas. 2015 was an *annus horribilis* for data breaches in healthcare, with more healthcare records stolen than at any other time since records started being kept in the United States. According to a 2016 mid-year summary on data breaches,[2] the trend is persistent: In June 2016, more than 11 million patient records were exposed in the United States and 2017 followed the same trend regarding the number of reported breaches, although the number of records exposed was lower than previous years.[3] **Figure 1** shows the status of worldwide data breaches from 2011 to 2017 as explained in the 2018 Italian Association for Cyber Security (Clusit) Annual Report.[4] The report collects data about known breaches worldwide from public sources. It is impressive to note the steep increase in healthcare breaches from 2015 to 2016 (up 103 percent), with a further increase from 2016 (73 events) to 2017 (80 events).

An analysis of data breaches shows they can be classified according to six main categories:[5]

- **Cybercrime hacking**—This is a common scenario, not necessarily involving high-level cyberskills. The easiest way to bypass hospital security is to spear phish workers, inducing them to click on malicious links.
- **Loss or theft of mobile devices and media**—Sensitive data are everywhere, quite often outside the IT-secured infrastructure. Mobile devices are, by nature, subject to theft and loss and, in many cases, the absence of encryption on the devices results in unwanted sensitive data leakage.
- **Insider accident**—A well-intentioned worker performs an action resulting in unauthorized access to sensitive data.
- **Business associate**—A third-party organization working for a hospital experiences a data breach involving clients' sensitive data.
- **Malicious insider fraud**—This is one of the more dangerous types of data breaches. It is often said that it is difficult to protect an organization from outsider attacks and almost impossible from insiders.
- **Insider snooping**—A worker accesses patient data without any legitimate need to do so.

Figure 1—Worldwide Data Breaches 2011-2017



Source: © Clusit—Rapporto 2018 sulla Sicurezza ICT in Italia. Reprinted with permission.

Other sources differ slightly on the classification and the wording, but all agree on these types of data breaches.

The likelihood of a data breach is correlated to the explosion of data. One industry expert estimates that the overall volume growth of data storage requirements in the healthcare sector is doubling every 18 months (another variation of Moore's Law[6]). The growth encompasses all types of data, from structured data in the electronic medical record (EMR) to unstructured and imaging data.[7] However, imaging and unstructured data, the worst condition from a security standpoint, are the real fuel of this data explosion.

> "WITH THE CONTEXT BEING SO CHALLENGING, THE CIO ROLE IS POTENTIALLY CRUCIAL FOR SECURITY IN HEALTHCARE AND FOR COMPLIANCE WITH THE GDPR."

Going beyond data breaches, there are software-controlled technology systems in healthcare (medical devices, automation systems, supervisory control and data acquisition [SCADA] systems, robotic systems) where a security issue for the controlling software could turn directly into a safety issue for patients. Healthcare organizations' reaction to such threats is usually to strengthen information and communication technologies (ICT) security measures, essentially reinforcing the power of the CIO over IT security. Truly, with the context being so challenging, the CIO role is potentially crucial for security in healthcare and for compliance with the GDPR. However, three paradoxes can undermine even the most sound security strategy.

Paradox 1: Are There More Things in Shadow IT Than in Official IT?

"There are more things in heaven and earth, Horatio, than are dreamt of in your philosophy."[8] It seems like "a long time ago in a galaxy far, far away"[9] when IT systems were confined to a well-defined number of applications managed by the IT department. It was a different time and, it seems, a different galaxy. Of course, non-IT departments (e.g., marketing, production, human resources [HR]) sometimes circumvented traditional IT and set up departmental systems. However, it was not so difficult, if needed and desired, to comprise such systems (often called shadow IT, or IT solutions not managed by the IT department) in official IT. For many companies, it was an unspoken strategy to let single departments "experiment" with local applications and then select the best solutions to be included in corporate IT. In a way, if a proper governance model was in place, IT never lost control.

Then the cloud came, with its powerful and fascinating stack of services: Software as a Service, Platform as a Service and Infrastructure as a Service. It represented a bounty of opportunities for users and departments to develop shadow IT solutions with unprecedented possibilities. The traditional IT department, as more often than not happens during a decisive revolution, applied the same governance model as the pre-revolution era, letting users experiment with new technologies and trying to capture the best of breed for corporate IT. Many IT departments are probably still pursuing this strategy. They scout the cloud for the best solutions, they use different cloud solutions themselves and they assume they know what their users are doing and why.

Here is a typical "hyperopia" problem, i.e., a common type of vision error where distant objects may be seen more clearly than objects that are near. An interesting Cisco report[10] states that IT departments estimate their companies are using an average of 51 cloud services. The same report evaluated that in an average company, 730 cloud services are actually being used. Another enlightening report was published recently by Logicalis.[11] The company interviewed 420 CIOs in Europe, North America,

Enjoying this article?

- Read *GEIT For Health Care. www.isaca.org/GEITforhealthcare*
- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-security-management*

Latin America and Asia Pacific with interesting results. Among the panel, 34 percent of CIOs stated that they can influence less than 50 percent of IT spending. In 2015, 66 percent of CIOs still had the ability to influence more than 50 percent of IT spending. It is interesting to note that this figure had fallen by 6 percent when compared to 2014 data.[12]

Paradox 2: In Healthcare, a Large and Growing Amount of Sensitive Data and the Most Dangerous and Potentially Life-Threatening Systems Are, From the Security Perspective, in a "No Man's Land" (Call It Shadow IT or Not).

If paradox 1 spans across virtually every market, things become more interesting when the focus moves to healthcare. Besides "official" IT managed applications, there are a number of critical information and automation systems usually passing undetected under the radar of IT departments, such as automation systems of different kinds and medical devices' data systems (MDDS). These embrace a broad perspective, taking into account both information and automation systems, since from the security point of view, they are both crucial. Automation systems are unevenly spread in hospitals, whereas MDDS are significantly present in every hospital.

Following is a short list of technological systems, which are usually software-controlled and network-connected systems, falling in a sort of "no man's land" regarding IT governance and security. Needless to say, these kinds of systems have a vast attack surface and potentially high risk:

- **Building automation systems (BAS)**—Most modern hospitals include "by design" systems to monitor and control lighting; heating, ventilation and air conditioning (HVAC); energy usage; security; fire; and elevators. In other cases, a complete or partial BAS infrastructure is installed over an existing hospital, including video surveillance data. Since hospitals are, more often than not, composed of many connected locations, the BAS infrastructure frequently controls a considerable number of buildings. A security attack on such a system could have a deep impact not only on hospital security, but on people safety as well.
- **Robotic systems**—The use of robotic systems is becoming a standard practice in some specialties. Probably the most famous is the Da Vinci Surgical System by Intuitive Surgical. A report offers a good starting point to grasp the concept of the diffusion of robotics, for example, in urology.[13] Both are US Food and Drug Administration (FDA)-approved devices, and both can be used in a network to support the "remote presence" of a physician or a surgeon.

> "INTERESTING SITUATIONS ARE EMERGING IN WHICH BUILDING/ROOM AUTOMATION, MDDS AND ROBOTICS CONVERGE IN A COMPLEX SCADA SYSTEM."

- **Medical devices and MDDS**—According to the FDA:

> *Medical devices range from simple tongue depressors and bedpans to complex programmable pacemakers with micro-chip technology and laser surgical devices. In addition, medical devices include in vitro diagnostic products, such as general purpose lab equipment, reagents, and test kits, which may include monoclonal antibody technology.*[14]

Nevertheless, the category of medical devices also includes highly complex electronic radiation-emitting products and diagnostic equipment. Examples include diagnostic ultrasound products, x-ray machines and medical lasers. Medical devices are broadly used inside and outside hospitals. Medical devices were historically stand-alone stations with no supervisory module. The subset of medical imaging devices normally connects via a picture archiving and communication system (PACS) to share imaging data, and laboratory systems have a dedicated automation and data management solution called laboratory information systems (LIS). PACS and LIS are well-defined objects subject to specific regulations and usually (but not always) managed by the IT department. Besides LIS and PACS, other medical devices are often equipped with MDDS, as defined previously, and this is a gray zone with respect to IT security. A data breach (or a loss of data integrity) on such systems can have significant consequences.

> “SOME IMAGING DEVICES MAY NOT BE EQUIPPED WITH ANTIVIRUS SOFTWARE, AND USUALLY THE OPERATING SYSTEM OF THE WORKSTATION ATTACHED TO A MEDICAL DEVICE IS NOT PATCHED REGULARLY (SOMETIMES IT IS NOT INCLUDED IN THE PATCH MANAGEMENT PROCESS AT ALL).”

Interesting situations are emerging in which building/room automation, MDDS and robotics converge in a complex SCADA system. For example, the Therapy Imaging and Model Management System (TIMMS) is a complex system to integrate and manage heterogeneous medical devices, clinical information systems and components of computer-assisted surgery in the operating theater.[15]

This example makes evident the convergence of IT with operating theater automation and medical device management. The consequence of this kind of technology evolution and convergence (which is not, of course, a negative trend in itself) is that the “no man’s land” is getting wider and wider, sometimes exceeding the land under the governance of IT or the clinical engineering department. It is not exactly shadow IT, since these systems are, in a way, official technologies, but from the security perspective, they are unmanaged systems in many hospitals, exactly as shadow IT is.

Going further, the medical devices managed by clinical engineering are a potential security threat as well. For example, some imaging devices may not be equipped with antivirus software, and usually the operating system of the workstation attached to a medical device is not patched regularly (sometimes it is not included in the patch management process at all). Moreover, bring your own device (BYOD) policies, applied in many hospitals without proper governance and risk limitation practices, and issues with implantable medical devices[16] pose new and unprecedented threats to security and safety in the hospitals. The recent field action by the FDA on Abbot Laboratories, requiring a firmware update to address cybersecurity vulnerabilities in implantable cardiac pacemakers, is a striking example of the level of security issues that exist in healthcare today.[17]

Again, the trend is more cogent in healthcare (where a security problem on a SCADA system controlling an operating theater could have frightening consequences), but it is analogous to what is happening with SCADA systems in other industries as well. A 2012 Accenture report provides an interesting overview of the phenomenon.[18]

Paradox 3: CIOs Are Working Hard to Fortify the Walls of the Citadel, but There Is no Citadel to Defend.

The traditional approach to IT security is focused on strengthening the security of IT systems. If this statement seems purely tautological (and it is), it is important to consider the implications. The previous paradoxes demonstrate that technology systems (IT or automation) outside IT department borders are growing and sometimes exceeding traditional IT systems. Moreover, in healthcare, the most vulnerable (and sometimes dangerous) systems are probably the ones outside the IT perimeter. Using a metaphor, IT professionals are spending a good

deal of their time and effort on security, fortifying a portion of the walls around the citadel of the patients' sensitive data managed by their hospitals. Yet, the idea of fortifying just a portion of a wall (e.g., leaving out the MDDS) is clearly ineffective, like a house where the main entrance is protected by an impenetrable security door while all the windows are open. Moreover, further exploring the analogy, the whole idea of a citadel protecting the sensitive data is outdated. In an ecosystem where traditional IT systems are coexisting with user-managed data (BYOD, shadow IT) and with a vast number of other data management systems (cloud, MDDS, SCADA), the protection of data and critical infrastructures must be addressed from a different point of view. The appropriate metaphor is probably an open city with a number of critical sites, not a walled citadel.

If it is still true that the majority of reported data breaches are still quite traditional in their approach,[19] it is likely that in the near future, cyberattacks will focus on the weaker part of the attack surface, i.e., the "no man's land" described in the previous paradox. A fictional depiction of what a cyberattack through medical devices might look like is narrated in the book *The Fifth Domain*.[20]

A New Paradigm

The paradoxes discussed support the need for a complete change in perspective. The (r)evolution can be articulated in four areas:

- Strategy
- Technology
- Processes
- People

Strategy

The first U-turn consists of redefining the vision of IT security, where a key point is to select the right analogy. As explained previously, the goal cannot be the defense of a citadel, but rather the protection of an open city with a wide attack surface. It is necessary to manage at a different security level and it is possible to even plan to secure or seal up portions of the city (critical buildings or infrastructures) when it is under attack, but walling the city is not an option nowadays. This is not far from the approach used to protect critical infrastructure. One interesting example of this approach applied to healthcare infrastructure is the Terrorist attacks on Hospitals: Risk and Assessment, Tools & Systems (THREATS) project,[21] part of the European Union's European Programme for Critical Infrastructure Protection (EPCIP).

The second U-turn is to move from a siloed approach (equivalent to fortifying a portion of a wall) to an integrated and holistic approach to security. All the information and automation technologies in the hospital must be addressed, regardless of who is responsible for what. A strategy purely focused on IT department borders is nonsense. Security must go beyond outdated borders and embrace traditional IT, cloud, clinical engineering, building automation, and all the subcategories of shadow IT that handle relevant and/or sensitive data or operations.

Technology

Technology can be an enabler of an integrated and holistic approach to security. This can be addressed in two directions:

1. In technology assessment and acquisition, it is important to ensure that security is one of the basic requirements, included by design in the technology under evaluation. This was straightforward in the past, but it is quite a challenge nowadays due to the manifold variety of technologies involved (traditional IT, user-acquired cloud services, medical devices, robotics and automation). The task of assessing new technologies cannot be accomplished by one department alone without coordination with IT and other technical departments. A clear example of the importance of a cross-border approach is the selection of an end-point security tool. Traditional antivirus software is a (partial) answer for end-user workstations, but in many cases, diagnostic equipment workstation producers will not allow IT to install antivirus

software. Actually, the solution is just around the corner: IT should select end-point protection software based on the integrity monitoring principle. The software will compute a hash code of the system files and alert the users (or the IT/clinical engineering departments) if the system files change compared to a certified baseline. This approach is a common technique used on SCADA systems, but it is often overlooked in healthcare because, since integrity monitoring is hard to apply to traditional clients, it is usually not included in the requirements the IT department considers essential for an antivirus solution.

> “THE POINT IS NOT TO HAVE THE BEST ANTIVIRUS, THE MOST EFFECTIVE FIREWALL OR THE TIGHTEST DATA LOSS PREVENTION (DLP) SOFTWARE, BUT TO BUILD THE BEST INTEGRATED AND MULTIDOMAIN-ENABLED SECURITY ARCHITECTURE.”

2. In selecting the tools and services (e.g., security operation centers [SOCs]) to support security, the IT department should incorporate an architectural vision more than a mere evaluation of a single product in a traditional best-of-breed approach. The point is not to have the best antivirus, the most effective firewall or the tightest data loss prevention (DLP) software, but to build the best integrated and multidomain-enabled (e.g., IT, clinical engineering and automation) security architecture.

Processes

Processes and methodologies must be updated as well. Presently, the IT department has a set of core methodologies for governance and security (e.g., IT Infrastructure Library [ITIL], COBIT® 5, International Organization for Standardization [ISO]/International Electrotechnical Commission [IEC] ISO/IEC 27001), while clinical engineering is working on a different set of methodologies (e.g., a health technology assessment [HTA]). This was fine a few years ago, when diagnostic equipment was purely machines. Now, the data-capture devices (such as medical devices with their MDDS) and automation technologies are mostly software-defined and software-controlled: A new methodology set and new processes are needed to guide the way new technologies are assessed, implemented and run.

People

People and organizational structures are among the crucial topics in every human endeavor. As this article has described, many healthcare organizations do not take into account the underlying technology convergence. The three typical technology departments in a hospital (i.e., facility, clinical engineering and IT) were born when buildings were walls and bricks, medical devices were dumb machines, and IT managed a well-defined set of applications and data. Now, buildings are Internet of Things (IoT) ecosystems generating critical and continuous streams of data, software-controlled robotic systems (ranging from logistic management to surgery) are both data generators and critical infrastructure components, and IT is scattered in hundreds of internal and external services. Many organizations are reacting with the establishment of a unified technology department. This is not a new trend: A 2006 article proposed convergence between IT and clinical engineering.[22] If a convergence between IT and clinical engineering is not possible, at least a chief information security officer (CISO) should be appointed, reporting directly to the chief executive officer (CEO), not to the CIO.

Furthermore, a cross-section of different skills and competencies should be the objective of every technology organization that aims to build a common culture and awareness about security themes. The 2018 Emergency Care Research Institute Report highlighted cyberattack as the top hazard for medical devices.[23] Therefore, IT professionals should be aware of the specifics of medical devices, and clinical engineers should be trained in the essentials of IT security.

The methodology frameworks (this time, for people management) should evolve. For example, the European Community is standardizing IT professional profiles around the so-called e-Competence Framework.[24] The framework is a landmark in digital competencies development, but a cross-professional approach that bridges ICT and clinical engineering (or ICT and plant automation, for more general contexts) is not yet included in the latest version of the framework.

Putting the Pieces Together

Setting aside for a moment the big issues with methodology and frameworks, there is a tangible path for hospitals and healthcare IT organizations that wish to address security and governance in a way that is aligned with the occurring technological convergence and with the accountability principle of the GDPR.

Taking inspiration from the Capability Maturity Model,[25] it is possible to propose a pathway in five stages (**figure 2**).

The stages can be defined as follows:

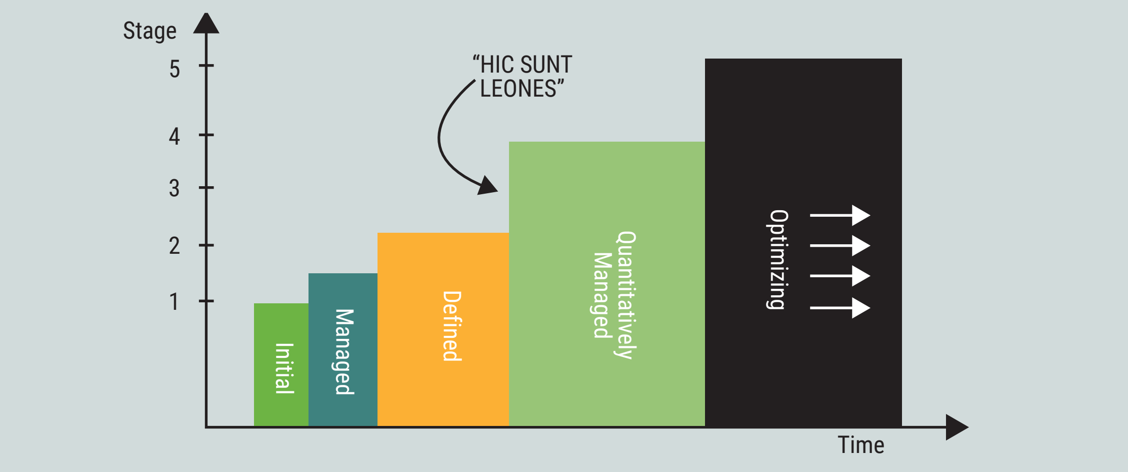
- **Stage 1 (Initial)**—"Local," not structured, security management exists.
- **Stage 2 (Managed)**—Structured security management for ICT is in place. There is general awareness about security in other technical areas (using the ICT department as the internal expert on call).
- **Stage 3 (Defined)**—Coordination efforts and policies on security are in place among different technology areas (e.g., ICT, facility, clinical engineering), but no dedicated cross-border organization for security exists.
- **Stage 4 (Quantitatively Managed)**—A cross-border role on security (e.g., the CISO reporting to the CEO) oversees security strategy and policies with a 360-degree approach. At the departmental level, security is well managed, with key performance indicators (KPIs) and monitoring processes.
- **Stage 5 (Optimizing)**—This is a converged security strategy and organization. The technology departments in the hospital are under a unified responsibility. Security and governance are managed with a holistic approach.

It is likely that any hospital, with due time and resources, could reach the Defined stage; going farther is more complicated. Reaching level 4 is more difficult ("*hic sunt leones*"[26]), since it requires a strong commitment and a cross-departmental approach.

If stage 5 seems too bold, it is worth considering this insight when discussing a broader context during a Cisco workshop:

> *IoT is made up of a Communications Internet, an Energy Internet, and a Logistics Internet that work together in a single operating system, continuously finding ways to increase thermodynamic efficiencies and productivity in the marshaling of resources, the production and distribution of goods and services, and the recycling of waste. […] Together, these three operating systems comprise the physiology of the new economic organism. The three interoperable Internets of the IoT require a transformation*

Figure 2—Proposed Five Stages of Holistic Security Management in Healthcare



> *in the functions of every enterprise. […] I expressed my doubts about the viability of chief information officers (CIO) in an evolving IoT economy and suggested that in the future, IT, energy services, and logistics would be integrated into a single function under the supervision of a chief productivity officer (CPO). The CPO would combine IT expertise, energy expertise, and logistics expertise with the aim of using the IoT to optimize the thermodynamic efficiencies and productivity of the company's operations.*[27]

This new holistic approach to security, governance and organization is the real game-changer. The cultural convergence of different professions, more than a pure organizational or technical convergence, is what will enable healthcare CIOs (and maybe other CIOs as well) to survive what can be defined as a perfect storm, or, from a more optimistic point of view, a perfect opportunity.

Endnotes

1 Heller, M.; *The C.I.O. Paradox: Battling the Contradictions of IT Leadership*, Routledge, USA, 2012

2 *HIPAA Journal*, "Major 2016 Healthcare Data Breaches: Mid Year Summary," *HIPAA Journal*, 11 July 2016, *https://www.hipaajournal.com/major-2016-healthcare-data-breaches-mid-year-summary-3499/*

3 *HIPAA Journal*, Healthcare Data Breach Statistics, *https://www.hipaajournal.com/healthcare-data-breach-statistics/*

4 Clusit, Rapporto Clusit 2018 sulla sicurezza ICT in Italia, CLUSIT, Italy, 2018

5 Houlding, D.; "6 Most Common Types of Healthcare Data Security Breaches," IT Peer Network, 18 February 2016, *https://itpeernetwork.intel.com/6-most-common-types-of-healthcare-data-security-breaches/*

6 A generally accepted computing rule stating that computer processing speed doubles every two years. Moore's Law, *www.mooreslaw.org/*

7 DeGaspari, J.; "Managing the Data Explosion," *Healthcare Informatics*, 1 October 2013, *www.healthcare-informatics.com/article/managing-data-explosion*

8 Shakespeare, W.; *Hamlet*, 1603

9 As seen in the opening sequence of every numbered film of the *Star Wars* series

10 Earle, N.; "Do You Know the Way to Ballylickey? Shadow IT and the CIO Dilemma," Cisco Blogs, 6 August 2015, *https://blogs.cisco.com/cloud/shadow-it-and-the-cio-dilemma*

11 Rogers, M.; "The Shadow IT Phenomenon," Logicalis, *https://www.us.logicalis.com/globalassets/united-states/whitepapers/cio-survey-2015-shadow-it-phenomenon.pdf*

12 *Ibid.*

13 Babbar, P.; A. Hemal; "Robot-Assisted Urologic Surgery in 2010—Advancements and Future Outlook," *Urology Annals*, 2011, vol. 3, no. 1, *www.urologyannals.com/article.asp?issn=0974-7796;year=2011;volume=3;issue=1;spage=1;epage=7;aulast=Babbar*

14 US Food and Drug Administration, "Is the Product a Medical Device?" USA, *www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm*

15 Lemke, H.; M. Vannier; "The Operating Room and the Need for an IT Infrastructure and Standards," *International Journal of Computer Assisted Radiology and Surgery*, November 2006, vol. 1, no. 3, p. 117-121

16 Pozza, G.; "Beyond BYOD: Can I Connect My Body to Your Network?" *ISACA® Journal*, vol. 5, 2014, *https://www.isaca.org/Journal/archives/*

17 US Food and Drug Administration, "Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (Formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication," USA, 29 August 2017, *https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm*

18 Sholten, B.; C. S. Filho; E. Smits; "Who Owns Information Systems in the Plant?" Accenture, 2012, *https://www.accenture.com/t20150624T211125__w__/in-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Industries_10/Accenture-MES-Who-Owns-Information-Systems-Plant.pdf*

19 Department of Health and Human Safety, Office of Civil Rights, "Cases Currently Under Investigation," USA, *https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf*

20 Pozza, G.; J. D. Halamka; *The Fifth Domain: Wake Up, Neo,* CreateSpace Independent Publishing Platform, 19 January 2014

21 THREATS, *www.threatsproject.eu/index.html*

22 Grimes, S. L.; "Convergence of Clinical Engineering and Information Technology," 24 August 2006, *http://accenet.org/publications/Downloads/Presentations/chime.pdf*

23 ECRI Institute, *Top 10 Health Technology Hazards*, ECRI, 2018

24 European e-Competence Framework, "ICT Profiles," *www.ecompetences.eu/ict-professional-profiles/*

25 CMMI Institute, *http://cmmiinstitute.com/*

26 "Here are the lions," meaning to say that this is the crucial point.

27 Rifkin, J.; *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, St. Martin's Griffin, USA, 2015