Exploring Information Security Risks in Healthcare Systems

Amy Ray
Bentley College, USA

Sue Newell
Bentley College, USA
Warwick Business School, UK

INTRODUCTION

The volume and severity of information security breaches encountered continues to increase as organizations, including healthcare organizations, struggle to identify more effective security policies and procedures. Publicly available guidelines such as GASSP or ISO17799 that are designed to facilitate development of effective security policies and procedures have been criticized for, among other things, inadequate attention to differences in organizational security needs (Baskerville & Siponen, 2002), and for inadequate attention to the social dimensions of security problems (Dhillon & Backhouse, 2001). In this contribution, we argue that the diversity of organizational security needs, as well as the need to recognize the social dimensions to security problems, will continue to grow as companies move away from employing unique, proprietary approaches to software and network development, in favor of adopting standards-based plug-and-play applications, and related standards-based methods and technologies designed to enable interorganizational as well as local systems interoperability.

We use complexity science and adaptive structuration theory to support our arguments that current security management policies and procedures focus on what technologies are used, and on planned systems use to the exclusion of unplanned—but real—emergent use and emergent development of systems. A more holistic approach to security that adapts to emergent systems developments—and most importantly, addresses alternative, emergent uses of systems—is needed, we argue. Throughout the article, we use examples from the healthcare sector to illustrate our points. We do this because Electronic Health Record (EHR) systems that will enable information to be shared across a variety of organizations (local doctors' offices, hospitals, health insurance providers, research organizations, and so on) and users (doctors, administrators, nurses, researchers, and so on) are at the early stages of adoption in many countries, so that much can be gained by starting with an informed view of what can lead to security risks, so that policies and practices are adopted that can protect the information that is being shared.

BACKGROUND

Software development has been described as a "craft" industry, because software applications are developed one at a time, and labor is by far the most significant cost of any development project. Various *standards*—or generally agreed-upon activities, methods, functions, protocols, interfaces, systems, equipment, materials, services, processes and products (De Vries, 2005)—have been introduced and employed in efforts to reduce the labor costs associated with IT projects, especially in terms of standards designed to facilitate creation of Web applications (e.g., TCP, HTML, HTTP, XML, SMTP, UDDI, SOAP).

These standards are generally referred to as Web standards or Web-based standards, and their power to provide interoperability between two or more systems has been established for decades. However, while these standards have benefits, it is important to recognize that using standards has an unintended consequence. More specifically, it can be argued that, as a result of *successful* use of Web-based standards for local systems development and systems integration, overall systems architectures are more complex, ultimately resulting in an environment of greater information security risk. In the next section, we explain why standards-based development and integration increase the overall complexity of the systems architecture, and subsequently consider

how this influences emergent use and architectural complexity, and so information security risk.

INFLUENCES ON ELECTRONIC HEALTHCARE RECORD SECURITY

IT Standards-Enabled Planned Systems Development and Complexity

At a local level, using IT standards simplifies the process of connecting one computer to a network of other computers. For example, employing Web standards, countless computers and computing devices around the world are connected, making the Web infinitely multidimensional and nonlinear. However, while Web standards simplify individual systems integration efforts, they potentially increase the complexity of the overall system architecture by enabling connections among heterogeneous systems.

Complex systems are defined as systems that interweave components in such a way that they display variation without being random, and result in a structure that is more than the sum of its parts (Lissack & Roos, 2000). Complexity science research has shown that many highly complex systems—including systems as diverse as the central nervous system, the biosphere, the stock market, telecommunications systems, and human immune system—are not only multidimensional and nonlinear, but are also made up of many selfsimilar components or properties that, in turn, enable development of more complex systems. EHR systems are good examples of such complex systems.

A number of healthcare data standards (e.g., medical code, individual and entity, and transaction processing standards) are now in place for electronic transmission of administrative data as a result of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Insurance claims data for a patient may be filed on a laptop computer or handheld device in a physician's office, processed by a claims manager from a terminal at an HMO, and otherwise accessed from any authorized device by a user with legitimate (or stolen) authorization. The challenge of mapping the network of authorized access points to HIPAA information grows as the network grows, and the network grows as the application of standards grows. In addition, in order to comply with HIPAA, many healthcare organizations have outsourced claims processing to healthcare clearinghouses (Ivans, 2003), increasing the complexity of the flow of data, as well as increasing the number of individuals with access to patient data. Thus, applying HIPAA transaction standards to systems integration efforts in healthcare simplifies the process of filing an insurance claim, but increases the complexity of the overall network architectures in healthcare.

Web Standards and Emergent Systems Development and Use

In an organizational or interorganizational context, Web-based standards are used to develop information systems applications in support of particular business processes. However, considerable research now exists which illustrates how actual use of IT is often different from the intended use. Users improvise by adding applications to the original system in order to support local practices (Ciborra et al., 2000; Pozzebon & Pinsonneault, 2005), and/or by simply using the system in ways not initially anticipated (Orlikowski, 2000). structuration theory (ST) (Giddens, 1979) and adaptive structuration theory (AST) (DeSanctis & Poole, 2004) are proven as useful frameworks for demonstrating how technologies are adapted and used by individuals within organizations. ST and AST address how social structures are changed via the interaction between a user and a technology, thus helping to explain the emergence and evolution of system use. In this sense, the real nature of a technology and its consequences emerge from the actions of individuals as they engage with and use the technology in practice (Orlikowski, 2000). These consequences can only partially be planned for in advance, and will vary across time and space as context, history, and process impacts the ways in which users develop knowledge through their reflective practice with the technology.

We again turn to healthcare to provide another example of this phenomenon. Since EHR are typically enabled by Web-based—as well as propriety—standards, and are employed by a highly diverse set of users, they are prime candidates for emergent development and use. EHR are designed to support documentation of clinical healthcare. However, physicians, researchers, nurses, insurance company employees, pharmacists, and many others are users of these systems, so it is reasonable to expect that different uses of the systems will emerge across user groups. For example, insurance companies are in the very early stages of adopting pay-