2018

Information Security: Going Digital

Richard Baskerville
Georgia State University and Curtin University

Recommended Citation

Baskerville, Richard. 2018. Information Security: Going Digital. Proceedings of 47th Annual Conference of the South African Computer Lecturers' Association SACLA 2018, 18-20 June, Gordon's Bay South Africa.

Proceedings of 47th Annual Conference of the South African Computer Lecturers' Association
SACLA 2018, 18-20 June, Gordon's Bay South Africa. Forthcoming in Springer LNCS.

Information Security: Going Digital

Richard Baskerville [0000-0003-2860-5215]

Georgia State University, USA and Curtin University, Australia
POB 4015, Atlanta, Ga. 30302-4015 USA
baskerville@acm.org

Abstract

Because "going digital" regards using digital technologies to fundamentally change the way things get done, information security is necessarily engaged in going digital. Society and science are going digital. For the sciences, this digitalization process invokes an emerging model of the science of design that incorporates the assembly of information systems from a wide variety of platform ecosystems. According to principles of bounded rationality and bounded creativity, this mode of design requires more creativity to develop needed functionality from a finite set of available platforms. Going digital requires more creativity in designers of all types of information systems. Furthermore, the designers' goals are changing. The traditional model of information systems is representational: the data in the system represents (reflects) reality. Newer information systems, equipped with 3D printing and robotics actually create reality. Reality represents (reflects) the data in the system. The paper explores the example of information security. Designers of security for information systems not only must be more creative, they must design for more goals. The security task is no longer just protecting the digital system, the security task is protecting the products of the digital system.

Keywords: Digitalization, Digital Artifacts, Information Security, Information Privacy, Information Systems

Introduction

Going digital is an expression with differing meanings. For some, it is simply a synonym for computerization: adopting a digital technology to communicate or process data. But in the business world, the expression has a deeper meaning. Going digital regards fundamentally changing the way things get done. Going digital creates new frontiers, new experiences, and new capabilities [1]. So inevitably, information security is going digital. This change in its nature does not imply that information security has not always been at least partly digital. It is meant to imply that the information being protected is going digital in a societal way [2]. It is also meant to imply that many things in the world are going digital, among them societal information; and information security is now charged with protecting them all.

Society is itself going digital. This unfolding event envelopes and engages myriad aspects of information systems research such as digital natives, digital immigrants, ubiquitous information systems, pervasive computing, inter-organizational information systems, IT diffusion and adoption, user acceptance of IT, mobile computing, enterprise systems, IT and new organizational forms, etc. [3].

As society goes digital, it is changing, and in keeping with this societal change, the reasoning about security also has to change. Such changes demand a fundamental rethink of the theoretical basis of information security [4]. A form of security reasoning has been common which could be regarded as security reasoning *around* the technology. As a result of the societal change, this reasoning must shift to security reasoning *through* the technology. In order to understand the shift in security reasoning, we will need to discuss what it means to be going digital with information systems.

The digitalization of society and science

Information systems is going through a thrilling period. The current period is thrilling because the rest of the world is discovering the marvels of digital technology. Society began going digital as mobile telephone technology began to operate in a digital mode. It quickly became obvious that information systems were being used as much for communications as they were for information processing. Many started using ICT (information and communications technology) as a term instead of IT (information technology). Soon after the availability of digital services on mobile telephones, together with the availability of personal computing, sparked the rise of myriad new kinds of applications: online shopping, online banking, social media, the Internet of Things, big data, FinTech, etc. As part of this emerging digitalization, science is going digital. Gradually evolving scientific disciplines have become more and more prominent. Examples of these new natural-science related disciplines included computational biology, computational physics, computational chemistry, computational neuroscience, and *in silico* medicine. Essentially every field of commerce, social engagement, science, knowledge, etc. has either digitalized or developed a digital counterpart.

The field of information systems has recognized that much of these digital developments have been focused on the notion of a digital device *broadly defined*. Such a digital device includes not just information processing, but networking, and software applications or apps. It is an integrated, often personal, information system within a single device. In the field of information systems, this recognition has led us to become interested in developing Herbert Simon's [5] original notions of the sciences of the artificial. This interest has developed in information systems as *Design Science Research*. Information systems recognizes that, as society goes digital, more and more human activities are organized with the aim of designing and creating digital artifacts. Thus the list of societal arenas and scientific disciplines that are now engaged in digital operations has expanded. These have quietly become, perhaps unrecognized by themselves, sciences of the artificial. Simon's original notions were based on an assumption that the natural sciences were different from the sciences of the artificial. The digitalization of the natural sciences is increasing making this assumption obsolete. For example with the development of biological science *in silico*, computational biology and laboratory biology are fast growing indistinguishable; merging into one discipline. Many logical experiments can take place within a computer. In this way digital biology is as much a science of the artificial as it is a natural science.

Digitalization and the science of design

Unrecognized here is that all of these scientific fields, natural or otherwise, are engaging in the science of design. That is, they are scientifically designing artifacts and studying the processes of design decisions. This form of design science constitutes the branch of design science research within information systems. This increasing engagement places information systems design science research in

a leadership position. This position could well serve as a model for the progression toward digital systems design in other disciplines.

These processes of design decisions have been consistently part of Herb Simon's work across his career. Simons work in decision-making is best known for what he called classical decision theory. Simon distinguished between classical decision theory and design decisions: "classical decision theory has been concerned with choice among given alternatives" [6, p. 172]. The decision process involved choosing from among alternatives that could be found. But design decisions are quite different. Design decisions have a degree of creativity. Design decisions are not only concerned with searching for alternatives but also through the elaboration of these alternatives. These alternatives were not just found, they were made: "design is concerned with the discovery and elaboration of alternatives." (op cit., p. 172) These design decisions actually guide subsequent search to a certain degree. Taking a design decision has the impact of confining future design decisions. It is a form of bounded rationality in which the boundaries are created piecemeal as a design progresses. Each design decision defines constraints on subsequent design decisions. If the constraints prove overwhelming, it is always possible to return to a previous design decision and rethink it. "The evaluations and comparisons that take place during this design process are not, in general comparisons among complete designs. Evaluations take place, first of all, to guide the search [, to] provide the basis for decisions that the designs should be elaborated in one direction rather than another." (Simon, 1972, p. 172.)

This means that designers create their own future design prisons. All designs are bounded by rationality. Bounded rationality means that individuals and organizations are limited by their collective knowledge, cognitive abilities, and the constraints of finite resources. But because our design decisions guide the search for future designs, and design decisions must be elaborated, design decisions are also bounded by creativity. Because one design decision constrains future design decisions, such constraints create a frame of reference, a confining box within which new design decisions must be taken. Whenever you have such a frame of reference, such as rational constraints, you actually have a more creative situation: all the constraints put new demands on human creativity in order to create solutions to achieve goals in a highly constrained environment [7, 8]. Individuals are known to be more creative when given operating limits [9].

The growth of digitalization means that there are growing creative demands being placed on people who are now engaged in digital design in all walks of society. These creative demands are actually stronger than those that were placed on the pioneers of information systems. This increasing demand strength is because the pioneers of information systems had such a broad range of design decisions that they could take; and they had so few constraints on these design decisions. But today designers and disciplines of wide variety are constrained by the existing consumer devices and platforms from which they must work. Their creative problem is, how to create a functional system that provides the means to their goals, out of the existing panoply of digital devices and platforms.

This problem is well-known. It is similar to the design of junk art. Junkyards offer domains of miscellaneous objects that have been thrown away, discarded, or sold for scrap. The junk artist assembles works of beauty from these *found objects*. They design and create junk art from the junk. While it is totally unfair to suggest that the marvels of the digital devices we have available today can be construed to be junk, the idea nevertheless is similar. The digital world is the domain of miscellaneous digital found objects that are available to consumers at very low cost. Across all walks of society and

science, we are now assembling marvelous information systems out of these found objects. It involves a higher degree of rationality, and a higher degree of creativity, because of the boundaries being placed on the ultimate designs by these pre-determined, and pre-defined objects.

The notion that today's computer information systems are junk art is not new. Such agile mash-ups are a return to notions of bricolage. Information systems bricolage is the pulling together of just the right kinds of digital technologies to solve the information problems [10]. In today's rapid digitalization of society and science, these found objects include digital platforms, ecosystems, apps, devices, etc. Our design task in information systems is to assemble useful information systems out of this constellation of digital platforms, ecosystems, apps, devices, etc.

Descriptive versus prescriptive information systems in a digital society

This progression of digitalization has not only changed the way we design systems, it has also changed the underlying systems themselves. Information systems have evolved. Yesterday's information system essentially processed the data into information which was then used by a human decision-maker. It was a simple four element system: Input data, the information system, the output information, and the decision-maker. See Figure 1.

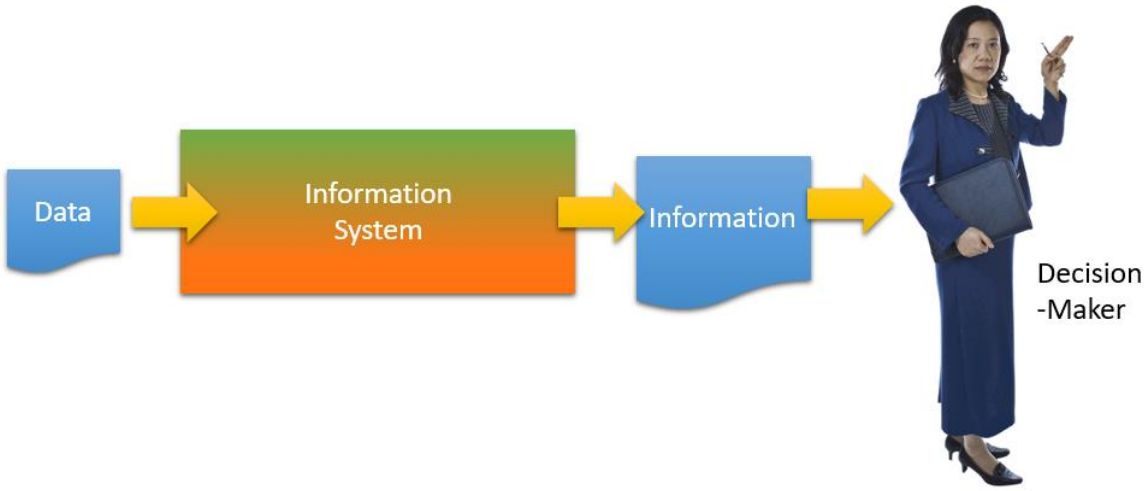

Figure 1. Early 4-element information system

Tomorrow's information system may be quite different. It is still a simple four-part system, but now it includes a decision engine that makes many of our decisions *in silico*. So the four parts are quite different in some cases. Sense, decide, instruct, and execute. (See Figure 2.) This revised system comes about because we have the Internet of Things to enable us to sense data as it is created (an event), we have artificial intelligence to make the decisions within the digital system, and we have robotics to actually execute, producing the system products without necessarily involving human actors. In this way the information system must be designed to go from events to products. The designs use found objects, and involve as little human interference as possible.

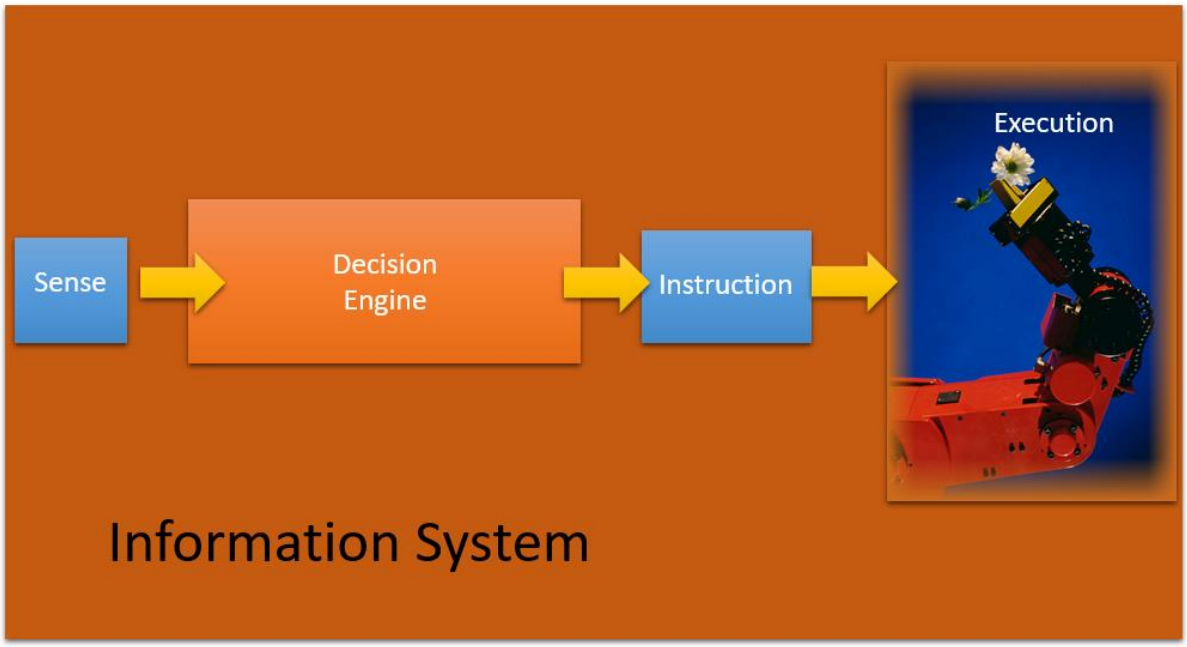

Figure 2. Emerging "Digital" Information Systems

Such information systems are not that far in the future. These newer kinds of information systems already decide what music we will hear and what movies we will watch. They do this by sensing our listening and viewing patterns, using artificial intelligence to decide what other music and videos we might wish to watch, and then executing these by offering us those digitally determined pre-selections for our enjoyment. With the increasing use of robotics and digital printing it is not impossible today to create similar systems that themselves create physical products as well as digital products. For such systems the stepwise process is sense, decide, instruct, and execute. The digital process runs from event to product.

As a result of this digitalization of information systems, many of our previous information systems research assumptions are inverted. Those assumptions included the notion that information systems were a representation of reality. For example, the data models are assumed to represent information about the world. They have a semantic relationship that is descriptive. Our notion of information quality relied on things like information accuracy, objectivity, timeliness, etc. These venerated research assumptions no longer hold in the digital world.

Our new assumption ground holds that information systems now create and shape reality. The real world is often a reflection of the system, not the other way around. This inversion arises because information systems create reality. They have a semantic relationship that is prescriptive. There is even an ethical dimension: is it morally proper to create the reality that is digitally determined?

The implications for information security are profound. Information security is no longer obligated to protect a representation of an existing reality. It is becoming an obligation to protect a representation of a future reality. The security task becomes one of protecting our next world. Information security,

then, is moving from protecting the digital assets and is now becoming involved in the digital consequences. In other words, today's information security is protecting not only the information system, but also protecting the products that it is producing. For security this is a means-end inversion. When information systems represented reality, that reality was the end, and the information system was the means. When information systems create reality, the information systems is the end, and reality is the means.

Security around the system versus security through the system

The previous mode of information systems, that of reflecting reality, defines the traditional information security goals of protecting the information and the system that produces it. But the newer mode for information systems, that of producing reality, forces us to ask, "What exactly are we securing?" Are we still protecting the computer system itself? If so it means the security concept is one of *providing a protection perimeter around the information system*. Alternatively we can ask, are we protecting the digital consequences of this information system? If the security concept is one of protecting not only the system but its digital consequences, its digital and physical products, then now we must think of providing a protection perimeter that encompasses not only the information system but also the products of that system. Security protects the products *through the system* rather than just *around the system*.

As a simple example, let us consider the Case IH Magnum autonomous tractor. (See Figure 3.) It is a driverless robotic tractor designed to be released into a field with whatever implements and attachments that are required for agriculture. The tractor does its work under computer control that is guided by electronic signals (such as GPS locations) and other Internet of Things devices. In previous times, the security mission would be that of protecting the computer system, and the security mission would seek to provide *security around* the computer system. The protection perimeter would extend around the computer, the communications network, and the various data input devices. It is security around the system.

Figure 3. Case IH Magnum Autonomous Tractor in field with a planter implement (from http://www.cnbc.com/2016/09/16/future-of-farming-driverless-tractors-ag-robots.html)

But with newer modes of digital systems, the whole ag-robotic tractor becomes part of the system. The tractor is conceptually the robotic endpoint of the information system. This incorporation of robotic output extends the protection boundary to include the robotic tractor as well as the other information elements. We would still provide *security around* computer system, the network elements and now the ag-robotic tractor. (See Figure 4.) But such security designs are made problematic because of the increasing use of platforms in the design. Security perimeters must account for the platforms and platform ecosystems that become involved in "going digital".

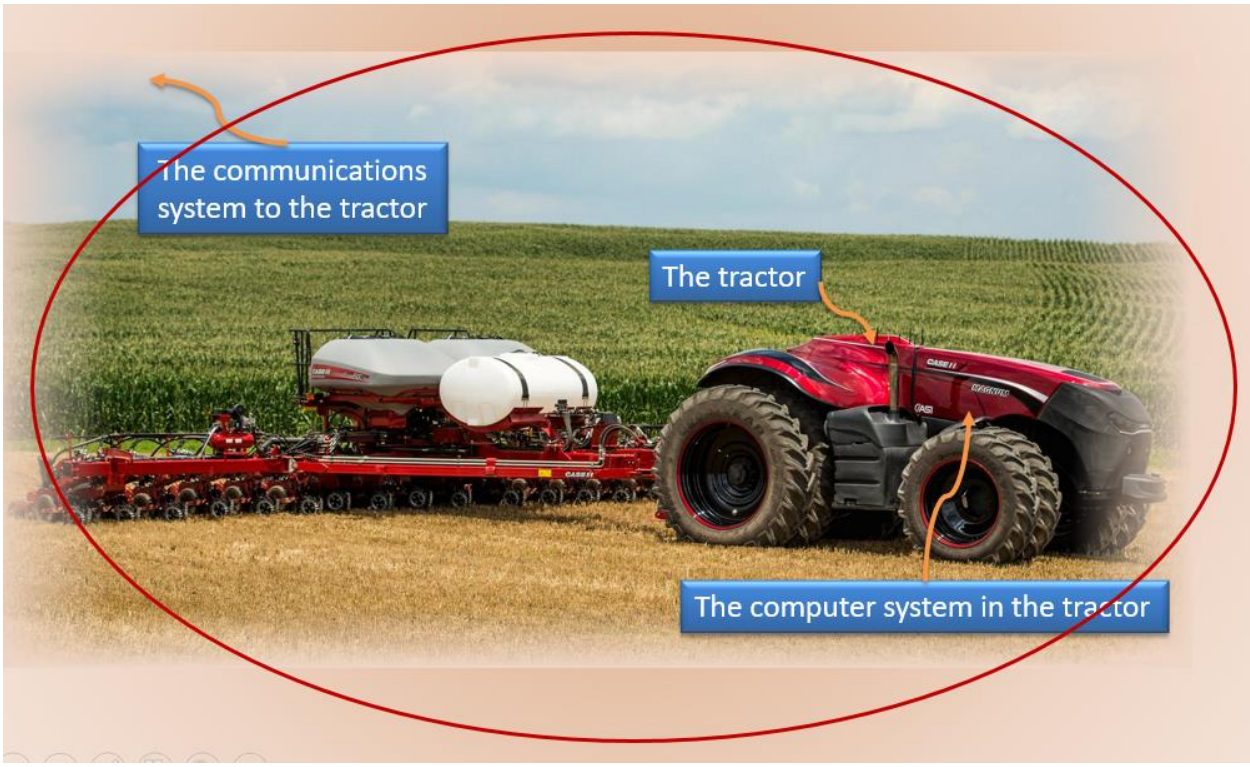

Figure 4. Security Around The System, protecting the tractor system.

However, this system is not a traditional information system in which the human decision-maker is receiving information. This artifact is an information system that is producing agricultural products. In this case, this information system (because of its links to sensors artificial intelligence and its robotics) is producing a crop. The information in the system is creating a crop. In this way the mission of information security is no longer just protecting the tractor, its computer, and its communications. Now, the mission of information security includes protecting the crop. It requires a reset in the goals of information security. Information security now has the mission to protect the crop *through* information security. (See Figure 5.) This shift is a dramatic extension of the mission of information security and extends the information security perimeter in order to protect the system products.

Figure 5. Security Through The System, protecting the crop.

For information security, going digital means a new set of design principles to guide the convergence of information security and the security of its product. The first of these principles is that when data integrity falls, so can the integrity of our reality. When data is irrationally changed in an information system, it can change reality in irrational ways. This consequence arises because reality is the product that is an output of this information system. Because this product may be either digital or physical, changing the data will change the real world. The result arises from the inversion of the system-reality relationship in that data is no longer representing reality, reality is representing the data.

For example, suppose we gain access to change the viewing history data for an online, on-demand entertainment system. If we can configure this history to indicate that a happy and peaceful community prefers angry and violent films, then the intelligence routine of the entertainment system may shift to one that suggests only angry and violent films to the community. As a consequence, angry and violent films may become ever so slightly more popular, and it may even be possible that the community itself becomes ever so slightly more angry and violent. Changing the viewing system can create a different reality.

Discussion

Going digital in information security also highlights how security is itself evolving into a digital construction. Information security is no different than other aspects of reality. This evolution means that security exists first in the digital world, and this digital existence creates security in the physical world. Such an evolution would mean that it is no longer possible to have physical security where there is digital insecurity. As a result of such logic, digital security is now security of the first kind. It is the antecedent of security in the other aspects of our world. Physical security such as locks, fences, gates, and burly guards may become ineffective if digital security is absent. They cannot operate correctly without operating digital security correctly first.

Unfortunately, it appears to be the current case that our digital security is growing less and less effective. We have tended to underinvestment in security, at least partly because simply measuring security is difficult [11]. While our dependence on digital security grows deeper and deeper, digital security is encountering more and more issues. Currently, these problems surface as the inability of our information systems to prevent privacy losses that are a consequence of security failures [4]. Digital perimeters are highly permeable and difficult to protect [12]. They are easily violated. There is also an asymmetry between the attacker and the defender that makes attacks on digital systems easy. We currently have few effective ways to adjust this asymmetry such that attacks become more difficult, more dangerous, more costly, and more work.

Conclusion

Future research is needed into ways to overcome such fundamental problems. The issues are in motion: both the issues of *what* information security is charged to protect; and *how* information security must go about protecting it. In terms of *what* information security is charged to protect, the security perimeter is moving outward. First, to incorporate the (multiple) platforms and platform ecosystems that are inevitably drawn into the digital system design. Second, to include the digital consequences of information systems. These consequences include an increasingly broad range of digital and physical products. In terms of *how* information security goes about achieving such protection, our security mode is shifting from one of security *around* the system to one of security *through* the system. More creativity is required on the part of the security designer because the platforms create more rational and creative boundaries, and because the goals of information security have grown.

Currently, the provision of security on the basis of reasoning around the system is growing less and less effective in proportion to the broadening demands society is placing on its information systems. Such a system only provides security for a representation of the world without providing security for the world that the representation creates. Reasoning information security through the system is growing more essential as we progressively increase our use of systems that create reality. Reasoning about the protection of the world that is being created by digital technology has potential to provide a more thorough approach.

References

1. Dörner, K., Edelman, D.: What 'digital' really means. McKinsey & Company (2015)
2. Yoo, Y.: Computing in everyday life: A call for research on *experiential computing*. MIS Quarterly 34, 213-231 (2010)
3. Vodanovich, S., Sundaram, D., Myers, M.D.: Digital Natives and Ubiquitous Information Systems. Information Systems Research 21, 711–723 (2010)
4. Anderson, C., Baskerville, R., Kaul, M.: Information Security Control Theory: Achieving a Sustainable Reconciliation between Sharing and Protecting the Privacy of Information. Journal of Management Information Systems 34, 1082 – 1112 (2017)
5. Simon, H.A.: The Sciences of the Artificial. MIT Press, Cambridge, Mass. (1996)

6. Simon, H.A.: Theories of bounded rationality. In: McGuire, C.B., Radner, R. (eds.) Decision and Organization: A volume in honor of Jacob Marschak, pp. 161-176. North-Holland Publishing Company, Amsterdam (1972)
7. Hoegl, M., Gibbert, M., Mazursky, D.: Financial constraints in innovation projects: When is less more? Research Policy 37, 1382-1391 (2008)
8. Ward, T.B.: Cognition, creativity, and entrepreneurship. Journal of Business Venturing 19, 173-188 (2004)
9. Finke, R.A., Ward, T.B., Smith, S.M.: Creative cognition: Theory, research, and applications. MIT Press, Cambridge, MA (1992)
10. Ciborra, C.U.: From thinking to tinkering: The grassroots of strategic information systems. The Information Society 8, 297-309 (1992)
11. Pfleeger, S.L., Cunningham, R.K.: Why Measuring Security Is Hard. Security & Privacy, IEEE 8, 46-54 (2010)
12. Griffy-Brown, C., Lazarikos, D., Chun, M.: How Do You Secure an Environment Without a Perimeter? Using Emerging Technology Processes to Support Information Security Efforts in an Agile Data Center. The Journal of Applied Business and Economics 18, 90-102 (2016)