

AGILE SECURITY FOR INFORMATION WARFARE: A CALL FOR RESEARCH

Baskerville, Richard, Georgia State University, 35 Broad Street NW, Atlanta, Georgia 30302, USA, baskerville@acm.org

Abstract

The context of information security is changing dramatically. Networking technologies have driven the global expansion of electronic commerce. Electronic commerce is increasingly engaging sophisticated advances like digital agents and web services. As a result of such advances, the information systems architectures that must be secured are becoming dynamic: shifting landscapes of changing vulnerabilities. At the same time, the threats in these landscapes are also becoming more sophisticated and dynamic. Information warfare is raising the stakes in information security by leveling intensive and highly novel threats against civilian systems. Information security researchers need to develop organizational approaches and methodologies that respond to this new context. The conflation of information warfare and short cycle development theories promises new information security practices. These approaches and methodologies would effectively lead to agile information security development. Agile information security development anticipates threats and rapidly deploys necessary safeguards in the context of shifting systems landscapes amid pervasive systems threats.

Keywords: Information systems security, information warfare, security analysis and design, agile methods, short cycle development, Internet speed.

1 INTRODUCTION

The purpose of this paper is to analyse the growing gap between the changing landscape of information systems and the management of information security. This gap promises to bring a continuing flood of system vulnerabilities, unless research and practice leads to new approaches for the rapid and continuous development of security safeguards. As an analytical argument, rather than empirical research, this paper contributes an important and overlooked research agenda for information systems scholars in the coming decade.

The thread of this analysis and argument can be summarized as follows:

- The argument is premised on the emergent nature of globally competitive organizations.
- The context of information security is changing dramatically. Two particular arenas are notable:
 - First, Networking technologies have driven the global expansion of electronic commerce. Electronic commerce is increasingly engaging sophisticated advances like digital agents and web services. As a result of such advances, the information systems architectures that must be secured are becoming dynamic: shifting landscapes of changing vulnerabilities.
 - Second, the threats in these landscapes are also becoming more sophisticated and dynamic. Information warfare is raising the stakes in information security by leveling intensive and highly novel threats against civilian systems.
- Information security researchers need to develop organizational approaches and methodologies that respond to this new context.
 - The conflation of information warfare and short cycle development theories promises new information security practices.
 - These approaches and methodologies may effectively lead to agile information security development and emergent security organizations.
- Such forms of information security development would anticipate threats and rapidly deploy necessary safeguards in the context of shifting systems landscapes amid pervasive systems threats.
- Important and timely research questions are shaped by these arguments, and provide a research agenda that holds promise for greatly improving information systems security and thereby enabling widespread new applications of information and communications technologies.

This analysis and argument is developed in the following 4 sections. Section two analyses the two important ways in which the context of Information security has become a more dynamic setting, leading to emergent vulnerabilities and threats. Section three describes the need for different forms of security organizations in order to respond to this new context. Section four concludes with examples of research questions that must be addressed for Information security to respond to these needs.

A key premise of this argument is the emergent nature of organizations and their information systems (Bergquist, 1993). Emergent organizational forms endure continual change, a state in which these organizations are constantly seeking stability, while never achieving it. The emergence is more complex than simple environmental adaptiveness, but rather involves organizational forms that interact with their context, continually remaking themselves in self-referential ways (Varela, 1984). Emergent organizations correspond well with dynamic environments, such as highly competitive markets, by maintaining continual agility. As a consequence, emergent organizations are necessarily unstable and, importantly from a security perspective, are often unresponsive to centralized or hierarchical control. Of course, to a degree, all viable organizations must be somewhat emergent. However, highly competitive and global

marketplaces have driven the need for increasing the tempo of organizational emergence in many government and corporate organizations, while information and communications technologies have simultaneously enabled large, complex, and global organizations to engage a faster pace of emergence (Truex & Baskerville, 1998).

This organizational emergence has led to more emergent forms of information systems development (ISD): Forms that respond to unpredictable organizational needs with activities that are also unique and unpredictable (Truex, Baskerville, & Travis, 2000). Such forms of ISD deliver information systems (IS) that emerge in concert with, and thereby in support of, organizational emergence. Emergent ISD forms develop systems not as a series of defined projects each having a clear beginning and end, but rather as continuous redevelopment of the entire organizational portfolio of systems. These forms manage and orchestrate systems development without a predefined sequence, control, rationality, or claims to universality. Often associated with agile methodologies, such development has been compared to “growing” information systems (a gardening metaphor) as an alternative to “building” systems (an engineering metaphor) (Truex, Baskerville, & Klein, 1999).

Agile methodologies (Cockburn, 2001), are known by various terms such as short-cycle-time development (Baskerville & Pries-Heje, 2004), and internet speed software (Baskerville, Levine, Pries-Heje, Ramesh, & Slaughter, 2003). Such methods involve high-speed software development for intensely competitive markets, military applications, or in response to fast moving technology. These methods offer an alternative that supplements slower, traditional software methods where organizational settings permit tradeoffs between speed and quality, scalability or maintainability. Over this premise on faster, concerted emergence of organizations and their information systems, a security gap can easily open as shifting vulnerabilities and threats gradually escape stabilized security safeguards.

2 CHANGING INFORMATION SECURITY CONTEXT

The context of information security is changing dramatically as organizations emerge at higher tempos. Vulnerabilities and threats also emerge as the organizations and their information systems are remade.

2.1 Technologically-driven Vulnerabilities

Rapid advances in networking technologies, together with the widespread access to networks, have driven forward fast-paced global expansion of electronic commerce. Organizations worldwide are participating as stakeholders in this networked commerce. This enormous participation enables rapid development and deployment of exciting new technologies as organizations seek to gain competitive advantages over their counterparts.

Recent examples of these sophisticated advances include digital agents and web services (Walczak, 2002). Digital agents operate with a certain degree of intelligence and autonomy to perform services across computing applications, platforms and networks. Web services enable computing software to be delivered as a service to be performed rather than an appliance to be sold, the software equivalent to selling the eggs rather than the chicken.

Digital agents and web services pose extremely dynamic security vulnerabilities (van der Merwe & von Solms, 1998). In both situations, organizations have to be able to place strong degrees of trust in software operating outside of their complete sphere of control. Where these agents and web services are actually or potentially under the control of other organizations (e.g., trading partners or government agencies), an organization’s Information security vulnerability landscape could rapidly change beyond its control. For example, digital agents might be made to perform

malicious acts, such as destroying data or crashing systems (Abouzakhar & Manson, 2002). As another example, web services could be corrupted in destructive ways, such as a credit card verification service that verifies fraudulent credit cards.

Still, such networked technological advances promise to enable IS developers to more rapidly construct and deploy new systems and new versions of systems. The resulting information systems architectures become more dynamic. The architectures become more fluid as these extend across networks and employ software components that have been developed, and are being controlled, by other organizations. This shifting and increasingly dynamic architectural landscape is also necessarily shifting and increasingly dynamic vulnerability landscape (Badenhorst & Eloff, 1994).

2.2 Subjection Threats

It is not by chance that information and communication technologies are of growing political interest. The increasing dependence on IS by so many important government, military, and commercial organizations means that these organizations are becoming increasingly vulnerable to disruption through the disruption of their systems (Garg, Curtis, & Halper, 2003). Thus information systems are becoming more interesting as targets of subjection. In terms of Information security, a *subjection threat* is one aimed at subjugating systems and their stakeholders by disabling or controlling these systems. Subjection threats are a demonstration of power over an organization (or a government), achieving subjugation by disabling or diverting the systems necessary to its function. Talented hackers have managed for decades, in small and large ways, to subjugate some of the information assets of mighty corporations by breaking into their critical information systems.

2.2.1 *The Usual Suspects: Vandalizing Hackers*

The same technologies that have empowered global economic commerce are also empowering hackers (and hacking organizations) to grow in their ability to subjugate information systems using powerful intrusion tools, distributed denial of service attacks, and malicious code like viruses and worms. Thus, at a time when the vulnerabilities are becoming increasingly dynamic, so too are the historical sources of threat (Schultz, 2002).

2.2.2 *Information Warfare*

The historical sources of threat, however, are being joined by more powerful parties who have more dramatic interests in systems subjection. These parties are military and quasi-military (e.g., revolutionary or terrorist) organizations engaging in warfare operations. In addition to empowering dramatic advances in managing and coordinating business operations, information systems have also empowered similarly dramatic advances in managing and coordinating military operations. Computers in battleground settings have enabled a precision in the military application of force that is considered to be a “Revolution in Military Affairs.” (cf. Bhalla, 2003) It has naturally followed that military organizations are rapidly developing techniques to attack and defend the valuable and critical advantages of these military information systems. The result has become known as information warfare, “Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.” Information operations are “actions taken to affect adversary information and information systems while defending one’s own information and information systems.” (DOD Directive S-3600.1, 1996, cited in Denning, 1999) This widely cited definition is important because of its distinction between information warfare, which is reserved for conflict, and information operations, which may be ongoing in peacetime as well as wartime (Jones, Kovacich, & Luzwick, 2002).

As a result of increasingly sophisticated information operations, specialists in military information systems are drawing considerable resources into the development of pervasive attacks and hardened defences for information systems. These operations take place in a new “battlespace” that includes information systems (Crilley, 2001). As a result, information warfare leads to the development of information operations that represent deeply sophisticated and advanced subjection threats. In order to remain effective in both defensive and offensive operations, those responsible for information operations must race to explore ways to exploit new information technologies using subjection threats. In this way, military organizations are driving forward the tempo in subjection threat dynamics, at least in the military battlespaces.

2.2.3 National Information Infrastructures

The information battlespace overlaps commercial information resources in many ways. Attention is mostly drawn to the infrastructures that enable the essential services that underpin a society, including energy, banking and finance, transportation, vital human services, and telecommunications. The information systems that are essential to the operation of these essential services are known as the national information infrastructures (The President’s Commission on Critical Infrastructure Protection, 1997). The motive for attacks on these infrastructures by military or quasi-military information operations include the disruption of national defence and war making capabilities, the distraction of defence resources from other parts of battlespace, and the undermining of public confidence in national leadership.

Most of the sensational reports of the current vulnerabilities of these infrastructures are overblown. These national information infrastructures are proving to be somewhat robust in the face of current information security threats (Verton, 2003). The various “hacker wars” that have erupted in the shadow of national confrontations have failed to produce any notable impact (Vatis, 2001), and have developed into something more like juvenile food fights than serious warfare (Berkowitz, 2003).

However, in at least one incident, concepts developed for information warfare have been applied in an attack by quasi-military information operations against national infrastructures. In 2000, pro-Israeli hackers attacked web sites belonging to the Palestinian Authority, Hezbollah and Hamas. The pro-Palestinian retaliation was a well-designed, phased information operation. The first phase took down government web sites (the Knesset, the Defense Forces, and the Foreign Ministry), the second phase attacked the banking and finance infrastructure (web sites belonging to the Bank of Israel and the Tel Aviv Stock Exchange), and the third phase attacked the telecommunications infrastructure (NetVision, the main Internet service provider) (Vatis, 2001).

Clearly, the high-tempo emergent threats arising from the development of information warfare operations are appearing on the horizon of commercial information systems. These are subjection threats that are likely to be brilliantly designed for surprise, coordinated attacks. It appears that the increasing vulnerabilities of information systems will lead critical information infrastructures into more vulnerable postures at just about the same time that the subjection threats become considerably more powerful and pervasive.

Information warfare is raising the stakes in information security by positioning intensive and highly novel subjection threats against several sectors of commercial systems.

3 THE SECURITY RESEARCH GAP IN INFORMATION SYSTEMS

Research in information and communications technologies are developing underlying security technologies that can be used in addressing the changing security landscape. For example, advanced firewalls and virtual private networking (VPN) can be used to fragment organizational

information systems into security compartments, and to extend a secure network architecture across unsecured public networks like the Internet. While these are useful tools, we lack research into techniques for applying these tools in dynamic environments, such as in high-tempo emergent organizations. Information security managers will need to manage an increasingly complex security architecture in support of an emergent organization. In order to provide the groundwork for such management, information security researchers need to develop organizational approaches and methodologies that respond to this new context by providing techniques for supporting “emergent security.”

Like its organizational counterpart, emergent information security endures continual change, a state in which the security architecture and the security organization are seeking stability, while never achieving it. The security organization (and its architectural product) also continually remakes itself in self-referential ways as it interacts with its context. Emergent security copes with the dynamics of organizations, shifting information systems architectures, and shifting vulnerabilities and threats by maintaining continual agility.

Driven by the emergence in its context, security organizations and security architectures are already somewhat emergent. However, it would be unfortunate if security managers continue to operate as if security architectures, security organizations, and their context were still stable. It will become increasingly difficult to respond to a high-tempo emergent security landscape with an unresponsive, monolithic security organization and architecture.

Research into emergent information security management can draw from at least two existing streams of research. These research streams include defensive information warfare and agile systems development

3.1 Principles of Defensive Information Warfare

Information warfare extends to both offensive and defensive information operations. The primary goal of these operations is the achievement of information superiority. Information superiority is the condition of acquiring, synthesizing, processing and sharing vital information to an extent greatly exceeding that of an adversary (Hall, 2003). Offensive information operations regard degrading or destroying the vital information systems assets of an adversary, and are generally of interest only in military operations. Defensive information warfare, however, includes information operations that are aimed at protecting the organization’s information assets. These practices are very similar to the security practices commonly found in many well-secured commercial organizations.

However, there is one substantial, conceptual difference. Defensive information warfare operations, like their offensive counterpart, regard the OODA cycle as a basic measure of their effectiveness. The OODA cycle, (observe, orient, decide, and act) is the basic measure of the responsiveness of a effective security unit. An effective unit will sense a change in its setting (observe), analyze the meaning and importance of this change (orient), determine an ideal strategy taking advantage of the change (decide) and then implement this strategy (act). Information superiority is achieved when the cycle times for this OODA cycle is markedly shorter than that of an adversary.

3.2 Principles of Short-Cycle Development

The importance of short cycle times is familiar in competitive ISD communities. This class of ISD approaches, including agile methodologies and internet speed software, engage the principle of shortened cycle times with somewhat similar goals to defensive information operations: Competitive (superior) information.

Research into short cycle time development shows that a package of at least five key practices characterize this form of development. These practices include a focus on completion speed, release-oriented parallel prototyping, adherence to a fixed architecture, negotiable quality, and an ideal workforce (Baskerville & Pries-Heje, 2004). These practices respond to at least seven agile principles: Accept multiple valid approaches, engage the customer, accommodate requirements change, build on successful experience, develop good teamwork, effective software development conforms to project environment constraints, prepare for unexpected consequences from innovation in software processes (Baskerville et al., 2003).

3.3 Conflating Information Warfare and Short Cycle Development Theories for Commercial Information Security

These short-cycle practices and agile principles enable systems developers to observe, orient, decide, and act in response to changes in their software system's marketplace. Observation is enabled by customer engagement, orientation and decisions are enabled by prototyping and a fixed architecture, and action is enabled by ideal teamwork, negotiable approaches and quality, and accommodation for change. The similarity between the principles and practices of short-cycle development and defensive information operations is intriguing. Further research would be in order to determine if the short-cycle principles could be used by information security managers to implement concepts from defensive information warfare in order to create agile, emergent information security.

Such research could demonstrate that information warfare theory and short cycle systems theory can be fused and extended as a basis for a new theory of emergent information security. This theory would support agile security development as a basis for construct a commercial OODA cycle enabling organizational information security managers to gain information superiority over the exploitation of emergent vulnerabilities by subjection threats. It appears promising that an agile, emergent security organization would be responsive to the dynamic vulnerability and threat landscape that future information systems are clearly going to find as their context.

Such agile information security development practices would anticipate threats and rapidly deploy innovative safeguards in the context of shifting systems landscapes amid pervasive systems threats. Research must empirically demonstrate that an alignment between information warfare theory and short cycle theory would operate against constantly changing vulnerability and threat constellations. The result would be approaches and methodologies that would effectively result in agile information security development.

3.4 Comparing Agile Security and Existing Approaches

The development of agile security approaches would likely continue the existing evolutionary path of existing information systems security development and management methodologies. Siponen (2001) provides a thorough review of these methods in a generational analysis. Siponen's first and second generations are characterised as *conventional approaches* and include checklists, risk analysis, formal models and management/evaluation standards. First generation approaches arise largely from practical experience. Siponen's third generation is characterised as *non-conventional* approaches, and includes security semantics, the logical design approach, the spiral approach, abuse case modelling, and the use of object-oriented, entity relationship, and data flow techniques for security design purposes. Third generation approaches arise from the application of concepts from computer science, database, and information systems disciplines in the development of secure information systems. Siponen's fourth generation, which he characterises as *IS Community Approaches*, includes sociotechnical methods and responsibility

modelling. Fourth generation approaches arise from concerns about the security and welfare of the social community involved.

In the analysis above, we linked the rising dynamics of security threats and the availability of short cycle time development approaches. The concept of responding to fast-moving threats with fast-moving systems adaptation falls readily into Siponen's third generation of non-conventional approaches. In this case, we are simply applying concepts from software engineering in solving a security problem. However, the underlying causal factors leading to the severity of the dynamic security threats is of a more social nature. Drawing in principles of information warfare represents a formulated response of defensive information warfare in the face of offensive information warfare. These factors more readily fall into Siponen's *IS Community Approaches* because of the relationship to national infrastructures, terrorism, international law and morality.

4 THE RESEARCH AGENDA

The analysis and arguments above has shown that the high-tempo emergence of organizations and their information systems is both enabled and endangered by the information and communication technologies involved. The security of these technologies is growing problematic because of the dynamics in both the constellation of information systems vulnerabilities and the threats being leveled against these systems. The conflation of defensive information warfare theory and short cycle development theory suggests a possible avenue for future research that may prove fruitful in developing new emergent forms of security safeguard development.

As a result of this argument, there is a research agenda that raises at least three key questions for information systems researchers.

Research Question 1: How can agile methods be used to generate effective security requirements?

This research question is a theoretical question leading to a theory formulation. Although this work is partly completed above, additional theoretical development is needed to draw specific methods and techniques from the conflation of information warfare and agile systems development theories. This question will address issues such as: Can the two theories be directly ported into commercial security development? Does the conflation of the two theories lead to practical methods and techniques? Exactly how must information warfare and short cycle development theories be extended or modified to shape an emergent security theoretical framework? Are new security organizational forms or particular kinds of specialists required to fit these theories?

Research Question 2: In what ways do these agile methods change the development of security requirements?

This research question follows research question 2, and is an empirical question leading to descriptive results. It addresses the security development experience under the light of the new theoretical framework. This question will address issues such as: Is security requirements analysis easier, quicker, or less thorough than more traditional approaches. Are multiple approaches to security development needed? Are the requirements definitions more flexible, more attuned to changes in security vulnerabilities and threats, or dependent on a standard information security architecture?

Research Question 3: How is the outcome of emergent security development different from more traditional forms.

This research question follows research question 3, and it is also an applied question leading to descriptive results. It addresses the ultimate success arising from the application of theory and practice in developing security safeguards for information systems. This question will address

issues such as: Do emergent security organizations detect sudden changes in vulnerabilities or threats better than more traditional security organizations? Do the short cycle security safeguards deploy faster than more traditional methods? That is, is the result a form of security that is indeed more agile? Is the security better because it is more responsive? Does emergent information security lead to fewer security incidents? Are emergent safeguards maintainable or are they throwaway artefacts? Is emergent security cheaper or more expensive than more traditional forms?

These three questions illustrate the primary research agenda that proceeds from the analysis and arguments linking high-tempo emergent organizations, the changing landscape of information security vulnerabilities and threats, and the conflation of information warfare and short cycle development in pursuit of better information security. Since systems security is recognized as an important consideration in future information systems developments, there is a clear avenue for important, timely, and badly needed research to investigate these questions.

5 SUMMARY

Global competition is driving commercial information systems to be increasingly emergent in the face of increasingly more sophisticated threats. There is a growing gap between these information systems and the management of their security. Vulnerabilities are rising as a result. New principles and practices are needed in the security management arena that close this gap. One promising solution is the development of new approaches for the rapid and continuous development of security safeguards. Such a solution might easily draw from developed bodies of knowledge in information warfare and short cycle time development for the purposes of building agile information security. As in the field of software engineering, however, this solution does not supplant existing security principles or practices, but instead provides a supplement or extension. Short cycle time software development is premised on a well-formed and durable architecture. Similarly, agile security methods will require a well-formed and durable security architecture. Traditional information security management principles will endure in order to continue protecting traditional systems against traditional threats.

References

- Abouzakhar, N. S., & Manson, G. A. (2002). An intelligent approach to prevent distributed systems attacks. *Information Management & Computer Security*, 10(5), 203-210.
- Badenhorst, K. P., & Eloff, J. H. P. (1994). TOPM: A formal approach to the optimization of information technology risk management. *Computers & Security*, 13(5), 411-436.
- Baskerville, R., Levine, L., Pries-Heje, J., Ramesh, B., & Slaughter, S. (2003). Is Internet-speed software development different? *IEEE Software*, 20(6), 70-77.
- Baskerville, R., & Pries-Heje, J. (2004). Short Cycle Time Systems Development. *Information Systems Journal*, 14(2), (forthcoming).
- Bergquist, W. (1993). *The Postmodern Organization: Mastering the Art of Irreversible Change*. San Francisco: Jossey-Bass.
- Berkowitz, B. (2003). *The New Face of War: How War Will Be Fought in the 21st Century*. New York: The Free Press.
- Bhalla, N. (2003). Is the mouse click mighty enough to bring society to its knees? *Computers & Security*, 22(4), 322-336.
- Cockburn, A. (2001). *Agile Software Development*. Reading: Addison-Wesley.
- Crilley, K. (2001). Information warfare: New battle fields, Terrorists, propaganda and the Internet. *Aslib Proceedings*, 53(7), 250-264.
- Denning, D. E. (1999). *Information Warfare and Security*. Reading Mass: Addison-Wesley.

- Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, 11(2/3), 74-84.
- Hall, W. M. (2003). *Stray Voltage: War in the Information Age*. Annapolis, Maryland: Naval Institute Press.
- Jones, A., Kovacich, G. L., & Luzwick, P. G. (2002). Everything you wanted to know about information warfare but were afraid to ask, part 1. *Information Systems Security*, 11(4), 9-20.
- Schultz, E. E. (2002). Is hacking up or down? *Computers & Security*, 21(2), 103.
- Siponen, M. (2001). An analysis of the recent IS security development approaches: descriptive and prescriptive implications. In G. Dhillon (Ed.), *Information Security Management - Global Challenges in the Next Millennium* (pp. 101-124). Hershey: Idea Group.
- The President's Commission on Critical Infrastructure Protection. (1997). *Critical Foundations Protecting America's Infrastructures* (Commission Report). Washington, D.C.
- Truex, D., & Baskerville, R. (1998). Deep Structure or Emergence Theory: Contrasting Theoretical Foundations for Information Systems Development. *Information Systems Journal*, 8(2), 99-118.
- Truex, D., Baskerville, R., & Travis, J. (2000). Amethodical Systems Development: The Deferred Meaning of Systems Development Methods. *Accounting, Management and Information Technology*, 10, 53-79.
- Truex, D. P., Baskerville, R., & Klein, H. K. (1999). Growing systems in an emergent organization. *Communications of The ACM*, 42(8), 117-123.
- van der Merwe, J., & von Solms, S. H. (1998). Electronic commerce with secure intelligent trade agents. *Computers & Security*, 17(5), 435-447.
- Varela, F. (1984). The principles for self-organization. In H. Ulrich & G. J. B. Probst (Eds.), *Self-Organization and Management of Social Systems: Insights, Promises, Doubts and Questions* (pp. 25-32). Berlin: Springer-Verlag.
- Vatis, M. A. (2001, September 22). *Cyber Attacks During The War on Terrorism: A Predictive Analysis* [White Paper]. Institute for Security Technology Studies at Dartmouth College. Retrieved, from the World Wide Web:
http://www.ists.dartmouth.edu/ISTS/counterterrorism/cyber_a1.pdf
- Verton, D. (2003). Blaster worm linked to severity of blackout. *Computerworld*, 37(35), 1,4.
- Walczak, S. (2002). Information security for agent-based WWW medical information retrieval. *Logistics Information Management*, 15(5/6), 393-400.