Rividium Whites - White papers on leading edge technologies

Formal Security Models and the Modern Organization

How Security Models affect Today's DoD Contractors

Andrew Bruce, CISSP, PMP, FITSP-D
CTO, RiVidium Corporation (http://www.rividium.com/)
andy.bruce@rividium.com

11 August 2010

Topic Summary:

- The problem statement; why worry about formality?
- Mapping security policies to formal models
- Looking to the future and formal security models

Section 1: Introduction

Our organization performs work for and stores information on behalf of customers in the federal government. Our customers demand security, reliability, and scalability both for data storage and data access. To achieve these goals, we apply various formal security models to ensure that the data and systems we run operate within well-defined security perimeters. In this paper we look at selected formal security models to see how they enable us to satisfy customer requirements, thus helping us to provide the best possible value to them. Specifically, we examine:

- Brief definitions and **key terms** of selected formal security models.
- Our organization's overall **security policy** ("statements outlining entity interaction, access control, protection methods, and remediation")[1] and how **security models** ("requirements for proper support of and implementation of a security policy")[2] affect our organizational **roles**.
- How we use the **Parkerian Hexad**[3] to guide our **security structure**.

We close this paper with our view of how we see computer security models adapting to future threats.

Section 2: Selected Formal Security Models: Definitions

Models are critical for organizations because, as Bishop says, they "provide[] a definition of 'protect'...and conditions under which the protection is provided."[4] Formal security models were developed starting in the 1970s to define mathematically provable computer system processing flows. The goal of all formal security models is to ensure that a computer system starting in a secure state remains in a secure state throughout every operation. In this section, we provide a very brief set of definitions for the reader's reference.

Subject – A person or process desiring to consume data or execute a function.[5]

Object - Data to be consumed (or functions to be executed) by a subject. This white paper itself can be considered an *object* currently being consumed by the reader (the *subject*).

Bell-LaPadula (BLP) – From 1973,[6] defines a data confidentiality protection model. Subjects must have both *clearance for* and *need-to-know about* objects. Objects have both a security classification (example: SECRET, TOP-SECRET) as well as a compartment (example: IRAQ, AFGHANISTAN). Key Phrase: "No read up, no write down."

Harrison, Russo, Ullman (HRU) – From 1976,[7] this model requires a defined (and finite) set of procedures that may modify the access rights of a subject to an object. It was an extension to the Graham-Denning model from 1972.[8]

Biba Integrity (BIBA) – From 1977,[9] similar to BLP but designed to protect data integrity. Subjects and objects have integrity levels assigned to them; subjects with a higher integrity level may not read objects with a lower integrity level. Key Phrase: "No read down, no write up."

Clark-Wilson (CW) – From 1987,[10] another data integrity model. It allows subjects to modify non-critical (*unconstrained*) data items directly, but requires the use of intermediaries (*transformation programs*) to modify critical (*constrained*) data items. Data updates are audited by a separate *integrity verification procedure* prior to final acceptance.

Brewer-Nash (BN, "Chinese Wall") - From 1989,[11] this model protects against conflict of interest by allowing objects to be associated with "conflict groups." Once a subject accesses any object within a conflict group, the subject may not access any other object within that same group. As an example, consider a marketing company employed by IBM, Dell, and Sun. Once a marketing manager accesses privileged data about any one of these companies, the system prevents her from accessing privileged data about any competing company.

Section 3: Security Policy, Security Models, and Organizational Roles

Section 3.1: Overview

Our organization's overall security policy provides the "concise, implementable, and enforceable"[12] instructions for how we conceive, design, build, and maintain our customers' projects. In analyzing these policies, we see that many of them map directly to key aspects of the formal security models defined above. Thus, we find that formal security models have a demonstrable effect on our business functions. Taking this one step further, each of our organizational roles exists to serve a business function; therefore, these roles also map to one or more security models.

Section 3.2: Security Policy Mappings within our Organization

At the top of our organizational ladder, we have our "C" (Chief) level officers, such as our Chief Executive Officer (CEO) and our Chief Operations Officer (COO). In our small company these chiefs wear many hats, but as a group their *most important role* is to embody the overall vision and forward growth of the company. Our CEO, COO, and CTO personally wrote our corporate security policy that formalizes the expectations we have of ourselves .

From a practical perspective these security policies map directly to our customers' requirements and expectations. In short, our policies allow us to create and sustain the stable business environment in which we can win our customers' trust, perform work for them, and build future business opportunities. In the table below, we highlight selected policies[13] to see how they map to the formal security models above.

Policy	Roles Affected	Assurance	Maps To[14]				
			BLP	*HRU*	*BIBA*	*CW*	*BN*
Ethics	All	Our customers can expect us to operate using the highest standards, and to put their					X

Policy	Roles Affected	Assurance	Maps To[14]				
			BLP	*HRU*	*BIBA*	*CW*	*BN*
		interests ahead of our own (avoid conflicts of interest).					
Acceptable Use	All	Our customers can depend on us to monitor and control usage of our corporate networks (example: prevention of protected documents from being uploaded to Google Sites).	X		X		
Information Classification	Data Owners	Our customers know that their data integrity and confidentiality levels are identified. Where we support multiple customers, their data is kept separate and we always work in their best interest.	X		X		X
Information System Audits	Data Custodians (Operators)	Our customers can rely on us to ensure data update correctness (for example, proper use of Clark-Wilson integrity verification programs) and to detect unauthorized data access.	X	X	X	X	X
Anti-Virus / System Security	Operations	Our customers can expect our secure systems to remain secure.	X				
Application Service Providers	Business Development / Operations	Our customers know that we vouch for the level of service and ethical behavior of our partner vendors. Our customers' protected data will remain secret, whole, and sand-boxed from potential competitors.	X		X		X
Regulatory Compliance	Legal / Operations / Development	Laws such as HIPAA (privacy) and Sarbanes-Oxley (accountability) will be addressed correctly.	X		X		X
Application Servers	Operations / Development	Secured system servers do not permit escalation of privilege, and implement a least-privilege work environment.		X			

Section 3.3: Summation

As can be seen from the short list above, our organization's overall security policy addresses a number of required functions and processes that require organizational roles to fulfill them. The formal security models, far from being abstract or purely academic, offer valuable guidance to us today as we implement sophisticated solutions for real customer problems. In fact, Zi et. al. have documented a thoroughly modern method for a *network covert timing channel* that ties back directly to BLP (and the TCSEC "Light Pink" book[15]) whereby unauthorized information is passed "using Video On Demand (VOD) traffic as the media traffic."[16] The formal security models live on!

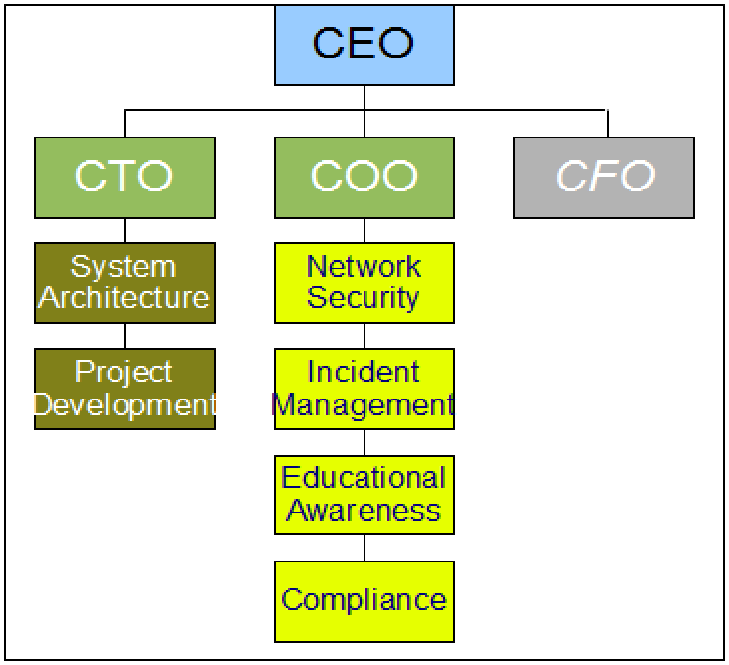
Section 4: The Parkerian Hexad and our Security Structure

Section 4.1: Overview

The Parkerian Hexad defines security in terms of *risk management*, particularly in how to address potential *loss scenarios*.[17] The Hexad defines six types of loss scenarios, three of which are contained in the classic CIA Triad (*confidentiality*, *integrity*, and *availability*) and three of which identify additional loss scenarios not truly covered by the Triad (*control / possession*, *authenticity*, and *utility*). These six loss scenarios (or, rather, their prevention) drive our organizational security standard; by addressing these concepts effectively we ensure that our security measures meet industry best-practices.

Section 4.2: Our Security Structure and the Hexad

In our small organization, we have the following high-level security structure:[18]



In this simplified picture, we focus on the Technical and Operations functions due to their hands-on security management requirements. While along with our CTO and CFO all of our company officers share legal accountability for security compliance,[19] only the CTO and COO functions perform day-to-day security oversight.

Section 4.2.1: Availability and Utility

The Hexad relates availability closely to utility; *availability* allows authorized users to access a resource while *utility* ensures that the resource satisfies a required business function. Our security structure primarily addresses availability through strong network management and incident response. Our network management helps by providing:

- Redundant power supplies as well as backup power sources for hardware
- Fault-tolerant disk storage devices such as RAID5[20]
- Strong application-level gateways that detect and defend against both external and internal security breaches

Our incident management team helps provide availability by ensuring that as security problems occur, we have documented plans for recovering from and continuing our business functions. In short, Disaster Recovery and Continuity of Operations for severe problems and a good Incident Response protocol to deal with (and recover from) all problems.

Section 4.2.2: Integrity and Authenticity

Integrity defines a consumer's assurance that a product (such as an email attachment) is complete, whole, and unmodified. *Authenticity* is closely related to integrity in that a product's source (such as the sender of the email attachment) is known authoritatively. Both are required for our organization's data to be acceptable to our customers and to ourselves. From a organizational security standpoint, these requirements permeate a number of structural areas:

System Architecture / Project Development – Projects that we build must be capable of proving their origin and verifying their contents. For example, software packages must be capable of reliably associating a specific product version with a given software release or our customers will be unable to manage the deployed software package effectively. We build systems with various checks (such as an MD5 check-sum) to prove that the systems have not been tampered with in any way.

Network Management – We use a PKI[21] to guarantee that messages we send to each other (example: email) as well as to our customers (example: product upgrades) are whole and from a provable source. Our PKI allows us to create *signing certificates* that can be used to generate a cryptographic check-sum that proves both that a message is unchanged as well as that a message truly came from its stated source. In accordance with NIST requirements, our certificates contain keys with a 2048 bit length and use RSA key pairs for signatures and key transport.[22]

Compliance – Our compliance group performs many types of audits to ensure that our environment meets regulatory and customer requirements. As an example of an audit that protects integrity and authenticity, our secure operating system log files are analyzed to detect unauthorized changes (such as modifications to critical operating system executable programs).

Section 4.2.3: Confidentiality and Possession

Confidentiality ensures that secrets are not revealed, regardless of how they are stored. *Possession* ensures that proprietary data and hardware remain firmly under our control. Our security structure addresses confidentiality in every aspect, with the most important element being educational awareness. Human beings are often the single greatest vulnerability to security breaches;[23] by educating our workers using proven strategies we can limit our possible exposures significantly.

Educational awareness – We provide employees with ethics training, acceptable usage policies, logon banners, Web safety programs, and social engineering protection resources. Employees must realize that information can be shared only with authorized individuals in authorized ways, when in doubt it is better to seek clarification. As a real-world example, using a social networking site to share information with a customer is *never acceptable* no matter how convenient it might be![24]

Systems Architecture / Project Development – Our systems must be built with strong security measures in place. As an example, personally identifiable information (PII) must be encrypted within storage files and the key strongly protected. Following NIST standards, we *educate users* to their key responsibilities and *prepare for a possible compromise* by ensuring that we can revoke keys and notify our customers.[25]

Network Management – We ensure that network communications are always encrypted. Additionally, we send confidential messages to email recipients encrypted with their PKI identity certificate to protect the message beyond the physical wire.

Compliance – By performing audits of our logical and physical assets (data and servers, for example) we ensure that we have retained possession and control of these assets. Plus, such compliance is essential to our business mission when we provide hosting services for customer-owned computing hardware.

Section 4.3: Summation

The Parkerian Hexad presents a well-defined set of loss scenarios that every organization must address. In our case, we find that *every element* in our security structure exists to mitigate one or more of these loss scenarios. Far from being a theoretical exercise, these loss scenarios identify both the problems as well as the proactive measures that we must take if we wish to be successful in gaining and maintaining our customers' trust.

Section 5: Computer Security Models and the Future

We have briefly reviewed how various formal security models apply to our organization. These models have stood the test of time to present proven methods of achieving a truly effective security posture throughout the enterprise. However, they are not the final answer by any means; our security needs expand in conjunction with the evolution of information technology itself, and our security models must grow likewise. Technology becomes ever more pervasive in our daily lives (consider that the Chipotle restaurant chain now has an iPhone app that allows online ordering[26]) and Coles-Kemp remarks that the “world is neither on- or off-line but a constant blending of the two.”[27]

The attack vector is changing rapidly, as cryptologist Bruce Schneier tells us: “only amateurs...still target machines; career criminals now target people.”[28] In a word, *social-engineering* where the stakes are literally a person's identity and available assets. To survive and prosper in this world, our organization needs to address this problem head-on. As Willett points out, “only recently has security become a legislative mandate.”[29] In his analysis on information assurance architecture, Willett goes on to list three extensions to the Parkerian Hexad: *privacy*, *authorized use*, and *non-repudiation*. Dlamini et. al. reinforce Willett's view with their report that ranks identity theft, privacy / regulatory compliance, and data protection as the *most critical* security issues.[30] Security is moving from an “operational and tactical level towards a strategic level of risk management,”[31] and companies must adapt to this environment.

While our risks are increasing, however, so are our options. The Department of Health and Human Services now actively reports privacy breaches, leading to more consumer confidence that if problems do occur then help is soon to come.[32] Cone et. al. posit the use of *video games* as an excellent vehicle for engaging employee situational security awareness and provide a working case study of the CyberSEIGE game developed by the US Navy.[33] And while the current economic climate makes employee fraud a higher risk, Hunt and Jackson provide a framework for *continuous control monitoring* that provides real-time assurance for all control points.[34] Finally, even mobile devices are moving toward a secure framework; a new security threat monitor for the iPhone[35] provides a list of latest threats and how to avoid them.

The key to successful security management in the future has one thing firmly in common with the past: it is our people who make or break security. As our own organization's information security model adapts to face emerging threats, we will continue to invest in educating, protecting, and partnering with our employees to maintain the secure environment our customers demand.

Reference List and Endnotes

Barker, Elaine, William Burr, Alicia Jones, Timothy Polk, Scott Rose, Miles Smid, and Quynh Dang. National Institute of Standards and Technology. *Recommendation for Key Management (Special Publication 800-57).* Retrieved July 27, 2010, from NIST Web site: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf.

Barker, Elaine B., William C. Barker, and Annabelle Lee. National Institute of Standards and Technology. *Information Security (Special Publication 800-21).* Retrieved August 1, 2010, from NIST Web site: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf.

Bell, D. Elliott, and Leonard J. LaPadula. "Secure Computer Systems: Mathematical Foundations" in *MITRE Technical Report 2547, Volume I*, March 1, 1973.

Biba, K. J., "Integrity Considerations for Secure Computer Systems," *MTR-3153*. MITRE Corporation: 1977.

Bosworth, Seymour, M.E. Kabay, Eric Whyne, eds., *Computer Security Handbook: Volume 1, 4th ed.* Hoboken, NJ: John Wiley & Sons, Inc., 2009.

Brewer, D. F. C., and M. J. Nash. "The Chinese Wall security policy" in *Proceedings of the 1989 IEEE Symposium on Security and Privacy*. IEEE Press, May 1989.

Clark, David D. and David R. Wilson. "A Comparison of Commercial and Military Computer Security Models" in *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP87)*. Oakland, CA: IEEE Press, 1987.

Coles-Kemp, Lizzie. "Editorial" in *Information Security Technical Report* 14 (2009), pp. 111-112. University of London: Information Security Group, 2009.

Cone, Benjamin D., Cynthia E. Irvine, Michael F. Thompson, and Thuy D. Nguyen. "A video game for cyber security training and awareness" in *Computers & Security* 26 (2007), pp. 63-72.

Dlamini, M.T., J.H.P. Eloffa, and M.M. Eloff, "Information security: The moving target," *Computers & Security* 28 (2009), pp. 189-198.

Dolan, Pamela Lewis. "Data breach reports now posted online," *American Medical News Online*. http://www.ama-assn.org/amednews/2010/05/03/bisd0504.htm (accessed: August 1, 2010).

Graham, G. and P. Denning. "Protection: Principles and Practices" in *Proceedings of the 1972 AFIPS Spring Joint Computer Conference*.

Guel, Michele D. "A Short Primer for Developing Security Policies." *The SANS Policy* Primer. The SANS Institute. http://www.sans.org/security-resources/policies/Policy_Primer.pdf (accessed: July 31, 2010).

Harris, Shon. CISSP All-in-One (AIO), 4th ed. New York: McGraw-Hill, 2007.

Harrison, Michael A., Walter L. Ruzzo, and Jeffrey D. Ullman. "Protection in Operating Systems" in *Communications of the ACM* 19, Issue 8, 1976.

Hunt, Richard and Marc Jackson. "An introduction to Continuous Controls Monitoring" in *Computer Fraud and Security*. June, 2010, pp. 16-19.

MacRumors. "Chipotle's Mobile Ordering App For Magic iPhone Burritos," *Gizmodo*. http://gizmodo.com/5129756/chipotles-mobile-ordering-app-for-magic-iphone-burritos (accessed: July 30, 2010).

National Computer Security Center. "A Guide to Understanding Covert Channel Analysis of Trusted Systems." *NCSC-TG-030 Version 1.* Fort Meade: MD, November, 1993.

Sophos.com. "Sophos releases Security Threat Monitor for Apple iPhone," *press release*. June 14, 2010 http://www.sophos.com/pressoffice/news/articles/2010/06/iphone-app.html (accessed: July 31, 2010).

Stephenson, Peter R., ed. *Information Security Essentials: Section 1*. Auerbach Publishing, ISBN 978-1-4398-0030-0, 2009.

Willett, Keith D. "Chapter 2: The IA^2 Framework," *Information Assurance Architecture*. Boca Raton: Auerbach Books, 2008.

Zi, Xiaochao, Lihong Yao, Li Pan, and Jianhua Li. "Implementing a passive network covert timing channel" in *Computers & Security* 29 (2010): pp. 686-696.

[1] Shon Harris, "Information Security and Risk Management," *CISSP All-in-One (AIO), 4th ed.*, (New York: McGraw-Hill, 2007), pg. 279. For space considerations, we paraphrase Harris' definition of a "security policy."

[2] Ibid, pg. 279. As before, we paraphrase the definition given in the text for a "security model."

[3] Seymour Bosworth, M.E. Kabay, Eric Whyne, eds., "Chapter 3.1: Proposal for a new Information Security Framework," Computer Security Handbook: Volume 1, 4th ed. (Hoboken, NJ: John Wiley & Sons, Inc., 2009), pg. 97. See the *Six Essential Security Elements* for a listing of the Parkerian Hexad.

[4] Ibid, pg. 277.

[5] Peter R. Stephenson, ed. *Information Security Essentials: Section 1* (Auerbach Publishing, ISBN 978-1-4398-0030-0, 2009), pg. 99. Retrieved on June 6, 2010 from https://norwich.angellearning.com/AngelUploads/Content/MSIA_2_0/_assoc/msia_s1/msia_s1_readings/ise_section_1_et.pdf. Our brief definitions of "subject" and "object" expand on the meaning given by Bell and LaPadula, as well as that given by Professor Matt Bishop in the *CSE* on page 279. We postulate that, in an Information Assurance context, subjects exist to *access* a function; conversely, objects exist to *satisfy* a function.

[6] D. Elliott Bell and Leonard J. LaPadula, “Secure Computer Systems: Mathematical Foundations,” *MITRE Technical Report 2547, Volume I* (March 1, 1973). Available online at http://www.albany.edu/acc/courses/ia/classics/belllapadula1.pdf (accessed: July 31, 2010).

[7] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman, “Protection in Operating Systems,” *Communications of the ACM* 19, Issue 8 (1976).

[8] G. Graham and P. Denning, “Protection: Principles and Practices,” *Proceedings of the 1972 AFIPS Spring Joint Computer Conference*, 417-429. This model (known as Graham-Denning) defines how to manage access rights governing actions (create, delete, read, and write) between a subject and an object. HRU adds the concept of protection based on commands rather than direct access, thus providing a level of abstraction and a function for the reference monitor (which mediates all accesses between subjects and objects).

[9] K. J. Biba, “Integrity Considerations for Secure Computer Systems,” *MTR-3153* (MITRE Corporation: 1977). Available online at http://handle.dtic.mil/100.2/ADA039324 (accessed: July 31, 2010).

[10] David D. Clark and David R. Wilson, “A Comparison of Commercial and Military Computer Security Models,” *Proceedings of the 1987 IEEE Symposium on Research in Security and Privacy (SP87),* 1987, Oakland, CA; IEEE Press, pp. 184-193.

[11] D. F. C. Brewer and M. J. Nash, “The Chinese Wall security policy,” *Proceedings of the 1989 IEEE Symposium on Security and Privacy*, pages 206–214, May 1989.

[12] Michele D. Guel, “A Short Primer for Developing Security Policies,” *The SANS Policy Primer*, The SANS Institute, pg. 27. Available online at http://www.sans.org/security-resources/policies/Policy_Primer.pdf (accessed: July 31, 2010).

[13] Interview with Chief Operations Officer, July 27, 2010. The policies listed here are a brief subset of the total security policies within our organizational plan.

[14] In this mapping example, we have abbreviated each of the formal models from our definitions section. We have made an attempt to explain *why* a particular policy maps to a given role and formal security model in the *Assurance* column, but space precluded a full description.

[15] National Computer Security Center, “A Guide to Understanding Covert Channel Analysis of Trusted Systems,” *NCSC-TG-030 Version 1* (Fort Meade: MD, November, 1993). The “Rainbow Series” of security books began with the “Orange Book” (the *Trusted Computer System Evaluation Criteria*, 1985; so-called because of its orange cover) to define levels of security from D1 (minimal protection) to A1 (verified design, the most secure system). The Orange Book did not account for network security, and was followed by the Red Book (“Trusted Network Interpretation”) in 1987. Future books were each distinguished by a different cover color. The text for the entire series of Rainbow Books is available from NIST online at http://csrc.ncsl.nist.gov/publications/secpubs/rainbow/ (accessed: August 2, 2010).

[16] Xiaochao Zi, Lihong Yao, Li Pan, and Jianhua Li, “Implementing a passive network covert timing channel,“*Computers & Security* 29 (2010), pg. 687.

[17] Bosworth et. al., *CSH*, pg. 97.

[18] Interview with Chief Operations Officer, July 27, 2010.

[19] Harris, *AIO*, pg. 891. As information assurance has become more of a legislative concern, senior executives must accept more accountability for security breaches. Harris provides both the Federal Sentencing Guidelines for Organizations (FSGO) and Sarbanes-Oxley (SOX) as examples of legislation holding executives accountable for company violations.

[20] Bosworth et. al., *CSH*, pg. 1501. RAID5 provides a highly available dist storage solution consisting of an “array” of *N*+1 storage disks; each of the *N* disks is used to store a redundant copy of the data. If a single disk in the RAID5 array fails, processing can continue unabated. Additionally, a replacement disk can be inserted into the array without forcing the machine in question to be taken offline (although performance degradation can occur as the new disk is synchronized with the other disks already in use).

[21] Stephenson, *ISE*, pg. 10. PKI stands for “public key infrastructure.”

[22] Elaine Barker, William Burr, Alicia Jones, Timothy Polk, Scott Rose, Miles Smid, and Quynh Dang, National Institute of Standards and Technology, “Part 3: Application-Specific Key Management Guidance,” *Recommendation for Key Management (Special Publication 800-57)*, pp. 26-27. Retrieved July 27, 2010, from NIST Web site: http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf.

[23] Harris, *AIO*, pg. 135.

[24] Anecdote from Chief Operations Officer, July 27, 2010. Apparently this was indeed the communication channel chosen by an employee for collaborating on a customer proposal during a crunch period.

[25] Elaine B. Barker, William C. Barker, and Annabelle Lee, National Institute of Standards and Technology, “Guideline for Implementing Cryptography In the Federal Government,” *Information Security (Special Publication 800-21)*, pg. 31. Retrieved July 27, 2010, from NIST Web site: http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf.

[26] MacRumors, “Chipotle's Mobile Ordering App For Magic iPhone Burritos,” *Gizmodo*, January 12, 2009, http://gizmodo.com/5129756/chipotles-mobile-ordering-app-for-magic-iphone-burritos (accessed: July 30, 2010).

[27] Lizzie Coles-Kemp, “Editorial,” *Information Security Technical Report* 14 (2009), pg. 111.

[28] M.T. Dlamini , J.H.P. Eloffa, and M.M. Eloff, “Information security: The moving target,” *Computers & Security* 28 (2009), pg. 191.

[29] Keith D. Willett, “Chapter 2: The IA2 Framework,” *Information Assurance Architecture* (Boca Raton: Auerbach Books, 2008), pg. 48.

[30] Dlamini et. al., “Information Security,” pg. 194.

[31] Ibid, pg. 195.

[32] Pamela Lewis Dolan, “Data breach reports now posted online,” *American Medical News Online*, May 4, 2010, http://www.ama-assn.org/amednews/2010/05/03/bisd0504.htm (accessed: August 1, 2010).

[33] Benjamin D. Cone, Cynthia E. Irvine, Michael F. Thompson, and Thuy D. Nguyen, "A video game for cyber security training and awareness," *Computers and Security* 26 (2007), pg. 64.

[34] Richard Hunt and Marc Jackson, "An introduction to Continuous Controls Monitoring," *Computer Fraud and Security* (June 2010), pp. 16-19.

[35] Sophos.com, "Sophos releases Security Threat Monitor for Apple iPhone," *press release*, June 14, 2010 http://www.sophos.com/pressoffice/news/articles/2010/06/iphone-app.html (accessed: July 31, 2010).