

Three Undocumented Layers of the OSI Model and Their Impact on Security

Michael Scheidell

President and Chief Technology Officer, SECNAP[®] Network Security Corporation

Synopsis

The single most serious threat to the security of sensitive information in today's world is not individual hackers, cyber gangs, inadequate firewalls or missing patches. The most serious threat lies in the often overlooked and undocumented OSI Layers 8, 9 and 10: Politics, Religion and Economics. These undocumented layers often drive sub-optimal decisions regarding information systems and data security, and can leave a program vulnerable to malicious intrusion or attack.

This paper seeks to help the reader understand how the traditional OSI model applies to security, realize that three additional layers exert a powerful influence over security programs and decisions, and leverage tips for navigating OSI Layers 8, 9 and 10 to become more effective security professionals.

Since founding SECNAP[®] Network Security Corporation in 2001, Chief Technology Officer Michael Scheidell has aggressively pursued the development of network security and email security products and services with impressive results, including patent-pending intrusion detection and prevention technology and a revolutionary email security product line. During the course of his career he has discovered and resolved vulnerabilities represented on the Common Vulnerability and Exposures (CVE) list, and has been a member of the FBI InfraGard program since 1996, working with other IT experts to assist the FBI's investigative efforts in the cyber arena.

Michael Scheidell and his talented technical team know how difficult it can be to affect positive change within an organization. When it comes to navigating the executive suite and the undocumented layers of the OSI model, the staff at SECNAP[®] Network Security have the experience and expertise to assist CIOs, CISOs and IT management in developing effective strategies to successfully drive security improvements.

The Most Serious Threat to Data Security is Not What You Think

The single most serious threat to the security of sensitive information in today's world is not individual hackers or gangs of cybercriminals. It is not an inadequate firewall, lack of logging or missing patches. Nor is the most serious threat to data security found in OSI Layer 7—no amount of application filtering or testing can address this threat.

The single most serious threat to the security of sensitive information lies in the often overlooked and undocumented layers of the Open Systems Interconnection (OSI) model: Layer 8 (Politics), Layer 9 (Religion) and Layer 10 (Economics).

You can conduct GLBA, SOX, FACTA, HIPAA, FERPA and ISO audits until you are buried in reams of audit reports. You can recommend implementation of DOD or NIST standards until you feel like Dilbert trying to convince his boss to do something logical. The bottom line is that, if your executive management is stuck in one of the hidden OSI layers—you are stuck as well.

This paper explores some of the issues unearthed during our security audits and offers insights to help you navigate the executive suite to overcome these issues. A quick word of advice: The last thing you want to do is present your executive team with a long list of recommended changes they won't read—let alone approve. Organizations fear change even more than they fear hackers. Pick your battles, and learn to suggest improvements in small increments rather than huge bites. This strategy will help you gain traction over time and build success in your role within the organization.

Beyond the Seven Layers

The traditional seven layers of the Open Systems Interconnection (OSI) model for network architecture begin with the most fundamental—the physical layer—and move upward in complexity through data link, network and transport layers, and on to session, presentation and application layers.

The seventh layer, application security, is two-pronged, encompassing web application security and email application security. Web application security addresses risks such as SQL injections and web-based attacks, while email application security focuses on viruses, worms and phishing. Most IT experts are trained to consider the seven OSI layers when making decisions regarding information security solutions. This is a fine construct, but is just a beginning.

These three undocumented layers of the OSI model exert a powerful influence on information systems and security decision-making. It is important to understand these additional layers, and how they can drive sub-optimal decisions, delay or derail projects, and open security gaps that can become security breaches.

The Scourge of Malware and High Cost of Cybercrime

The evidence is all around us. Cybercrime is rampant, ongoing, and expensive. Estimates by the Federal Bureau of Investigation suggest that cybercrime costs U.S. businesses a staggering \$67.2 billion annually. In its July 2007 report, the Federal Trade Commission declared that spam—spam!—has become a substantial global tool in the propagation of financial crimes. And when the Internal Revenue Service published its 2008 report on the 12 most serious tax scams, phishing topped the list! Phishing is a prime tool in the exploding problem of identity theft.

We are all familiar with the growing body of knowledge surrounding email communication, and the spyware and malware that can plague it. As of October 2007, for example, almost 70 percent of email communications sent to businesses were spam, according to Gartner research. (In residential households spam constituted 75 percent of all email received.) Research conducted by market intelligence firm IDC revealed that 10 of every 12 email messages are spam (83 percent), and one in 39 carries a virus. IDC also projected that consumers and businesses will spend more than \$305 million to detect and eliminate spyware between 2007 and 2011.

These numbers tell a disturbing story about the high cost of cybercrime. Among those costs are application costs such as the erosion of network bandwidth, reduced network performance and diminished network storage (that malicious email has to be quarantined somewhere!). There are the costs of lost employee productivity during hacker attacks or in dealing with destructive

worms and viruses, and time wasted by technical help in remediating intrusion-related issues. There is also the inestimable cost of a system compromise due to the carelessness of just one employee—which affects not only the bottom line, but also a company’s reputation and credibility among customers and partners alike.

How expensive is the perception among an organization’s stakeholders that the business may be vulnerable to attack? What is the cost of lost business? Recent news stories describe a seemingly endless series of network attacks on retailers in which sensitive customer data has been compromised. In response, embarrassed businesses are providing affected customers with free credit record monitoring services in an effort to protect them against identity theft. This is a bit like closing the barn door after the horse has escaped. Unfortunately, in most cases fines have yet to be imposed on the negligent businesses, but that pattern is expected to change.

There is little doubt that the cost of cybercrime has burgeoned in recent years and will continue to rise. According to Irida Xheneti, a research analyst for IDC's Security Services program, “The sophistication of the threat landscape, stringent regulatory mandates, the complex technology environment, and the potential impacts that security vulnerabilities present to corporations will force companies to invest heavily in IT security.” Other voices echo this projection.

Regulation and Responsibility

The Fair and Accurate Credit Transactions Act of 2003 (FACT Act) requires that a wide range of organizations—from banks and mortgage brokers, to telecom, gas and electric utilities, to automotive dealers—take serious steps to safeguard electronic transactions and credit information. The Red Flag rules, which must be implemented by November 2008 under the FACT Act, impose requirements on those organizations to proactively monitor transactions in order to detect and prevent abuse.

The Gramm-Leach-Bliley Act (GLBA) of 1999, Sarbanes-Oxley Act (SOX) of 2002, Health Insurance Portability and Accountability Act (HIPAA) of 1996, Family Educational Right to Privacy Act (FERPA) of 1974 and the over-arching Privacy Act of 1974 and subsequent amendments all impose privacy and protection requirements and most include penalties for non-compliance. To date, there has been no tendency to levy those penalties, although that pattern may change as security breaches continue to be publicized.

Gartner suggests that CIOs must manage IT risk as a business risk. Most security engineers, when performing risk analyses, use the seven OSI layers as a reference point for each link of the chain that needs protection. For example, the application layer must have properly coded programs to prevent bugs from allowing unforeseen problems, such as exploits or faulty programs, to compromise a network. OSI provides the cornerstone for interoperability and communications decisions. This is why, when we are faced with information technology purchasing decisions, we evaluate the functionality a product will deliver in addition to the OSI layer in which it will operate. However, what is generally not taken into account on a conscious level—although they may be significant factors on the sub-conscious level—are the three additional OSI layers and the role they play in the IT decision-making process. By failing to be cognizant of these additional layers or, worse, ignoring them, we increase our risk of sub-optimal decision-making.

In its Special Report in April of 2008, CIO Magazine addressed these “hidden” layers of influence as they impact medical care inside California prisons. The problem? Substandard medical care kills one inmate every week—in large part due to the absence of medical records, inadequate medical data, and lack of access to online medical references. The solution? Information technology was an integral part of a court-ordered prescription to ensure that prison doctors do no more harm. The report concluded, however, that progress has been slow, and that “doing IT behind bars requires overcoming physical, political and cultural obstacles foreign to most CIOs.” The hidden layers begin to be revealed!

OSI Layers 1 – 7 and Their Role in Security

Before we investigate the additional OSI Layers 8, 9 and 10, let’s examine two of the traditional layers of the Open Systems Interconnection model. Much has been written about the elements of each of these seven layers, and the SANS Institute has published an excellent article about applying the model to Information Security, including the relative merits of single-layer versus multi-layer security solutions at these layers.

Our security audits continue to confirm the existence of security issues in these layers and the importance of building security into each layer from the ground up. The following examples illustrate security gaps, encountered during our audits, in the lowest and highest layers of the basic model.

Layer 1 – Physical – The door to the server room is propped open for convenience during maintenance work, when the requirement is that this door be closed and locked to restrict access to this secure space. Another example we’ve all been victims of is the hard disconnect caused by the network guy tripping over a critical cable.

Layer 7 – Application – Your business is protected by a firewall that inspects the content of incoming packets. This firewall application must also be secured, by programmers observing software development life cycle best practices. A security gap or oversight may cost you \$1 to fix while you are writing code, but will cost \$100 to fix after a quality audit. And the cost of that security oversight will be immeasurable in the event of a future security breach.

Despite best practices applied in adding security to OSI Layers 1 through 7, the real devil is in Layers 8, 9 and 10, as we’ll see.

The New OSI Construct

Layer 8 – Politics

The eighth layer of OSI becomes evident when technology meets a decision-making process that is not entirely in the hands of the users. When all previous layers have been addressed, compliance issues may remain in an organization due to political blocking, which is generally the result of executives or board members who do not fully comprehend the ramifications of the underlying decision or the technical issues in play. However, they are the final decision-making authority, and tend to cross-pollinate with other executives both within and outside the company. Following are some examples.

At one publicly-traded bank, a Gramm-Leach-Bliley Act (GLBA) compliance audit discovered severe breaches of compliance laws that exposed the organization to attack as well as possible leakage of customer data. The incident was thoroughly documented, with remediation recommendations formulated and presented to the Director of IT, who agreed with the findings. However, the C-level executives were not convinced the problem warranted remediation because there had been no previous repercussions. Two months later, the company was victimized by a successful Denial of Service (DoS) attack, which took their systems offline for two hours and cost an estimated \$1.2 million. The Board of Directors subsequently directed that the audit recommendations be implemented as soon as possible—a good decision—but the genie was out of the bottle and it took weeks for the negative media exposure to wane.

In another example, a project team conducted an exhaustive evaluation of a software product to identify the “Must Haves” and “Want to Haves,” rank them, and narrow the search to three vendors. The team then evaluated the three vendors and ranked them as well. The lowest-ranked vendor provided the team with a product demonstration, during which the project team asked pointed and probing questions that should have resulted in elimination of that vendor. Unknown to the team, however, one of the vendor’s executives had a personal relationship with the executive to whom the project team reported. As happens frequently, discussions occurred above the team level to assure a decision in favor of that “preferred” vendor. Thus, while the project team comprehensively reviewed and evaluated the vendors and recommended a purchase decision in favor of the top-ranked vendor—justified by all the right evidence—the real decision was made at the next level and for reasons having little or nothing to do with OSI Layers 1 through 7. Instead, politics ruled this decision. As anticipated, the product chosen by the politically-motivated executive was difficult to implement and never really met expectations. Later, when the user community began to identify implementation issues, the project team was blamed even though it was not the team who had made the ultimate call. Layer 8—the political layer—had caused the decision to be redirected to a sub-optimal path.

Many employees of a certain private educational institution preferred short, easy to remember passwords, and because of their tenure had resisted changing their passwords. A password audit was performed to check for easily guessable passwords, and these particular passwords made the hit list. We suggested that the institution make users aware of their new complex password policy and establish a deadline for password expiration. To give the policy teeth, the IT team required approval from the president to ensure his support of policy enforcement—which they obtained. It was a small and modest beginning, to be sure, and stronger authentication methods would be preferable. However, implementing the one policy improvement they were able to is an important step, and it won’t be the last action the institution takes to strengthen its information security program.

In another case, a high-ranking executive allowed a visiting vendor friend to use an empty office and plug into the local network to catch up on her email between meetings. It turned out that the vendor’s machine was infected. Fortunately, the problem was detected quickly and the vendor was directed to remove her laptop from the network. The policy override that occurred at the political layer, however, created a security incident that could have had severe consequences had it not been detected so quickly. Later, a policy was approved—by the same executive—requiring visitors to acknowledge that they were not to connect laptops to the company network without approval and verification that their machine was up-to-date with all current patches. Other companies have experienced similar security incidents and have

implemented MAC address security on selected ports and in vulnerable areas such as conference rooms.

In another example, a small organization was permitted to share office space with a larger company, whose respective CEOs were friends. As an advance precaution, the larger firm implemented MAC address filtering on its network ports to prevent potential “cross-pollination” of malware from the smaller firm. This security precaution proved its value quickly, for the smaller company (which had no such filtering) had been infected by a visiting salesperson’s computer. As a result, several of their computers had become infected and were being used in a spam bot network. Since they also had weak outbound firewall rules, the smaller firm was unwittingly spewing spam from its email addresses, which caused them to be blacklisted by various email filtering programs and unable to send even legitimate email from their addresses.

As a final example (although there are hundreds more), imagine a publicly-traded company whose CFO often takes home his laptop in order to work in the evening. Of course the laptop contains some of his company’s financial data. Not unusual, and nothing to be concerned about, right? Not quite. As a C-level executive, he had invoked his executive privilege and obtained admin rights on his machine for his convenience in various job-related responsibilities. One evening, he allowed his teenage son to use the laptop. The son installed peer-to-peer file-sharing software, thinking so little of the action that he never mentioned it to his father. Subsequently, the CFO was faced with the very real prospect that the company’s financial information was able to be shared with others. The political layer allowed the CFO to override security policy and—because he works for a public company subject to Sarbanes-Oxley requirements—he could incur financial liability for having overridden that policy in the event the information became compromised.

Layer 9 – Religion

It may not occur as routinely as the experiences with OSI Layer 8 described above, but Layer 9—what we call the religious or faith-based layer—can have as much impact or more. In this layer, the decision-making process makes a leap from objectivity and fact-based considerations to allow the selection of a specific supplier, almost as if the decision-maker was hard-coded to that supplier. Vendors such as Cisco, Citrix, Microsoft, SAP and others, through rich budgets and even richer marketing initiatives, have created an aura of entitlement that results in decisions being made to select their products based on faith. They are the first (and sometimes the only) to be considered and are the easiest to sell to C-level executives. After all, “No one ever got fired for buying IBM,” as the axiom goes. No harm, no foul!

Faith-based decisions contributed to the wild-fire spread of Token Ring networking when Local Area Networks were first gaining traction. No doubt more than one project team was directed to evaluate LAN technologies and recommend the best option for the business—as long as it was Token Ring. Management was fanatical about IBM and they were not about to change their religion. However, time proved that the mainstream or most popular solution is not always the best answer. Eight years later Token Rings had been supplanted by Ethernet, but the religious layer had already done its work. We can only imagine what new and alternative technologies might have sprouted during that time, absent the powerful influence of nearly universal faith in a single vendor or product.

There are IT shops that employ only Microsoft servers, and those that only use Unix-based servers. And, yes, there are some sound economic reasons for standardizing on a particular platform or operating system. However, sometimes technology exists on one operating system that doesn't exist on another, or it may be less expensive in terms of labor or licensing to use one system over the other depending on the business functions to be supported. It is easy to become comfortable with the operating system we "grew up with" rather than one that objectively makes sense as a solution for the organization. Change is difficult. Change consumes time. Change requires investment. On the positive side, however, change can produce exciting new applications and tools. Change can jump-start new thinking. And if necessity is the mother of invention, change is the father.

In the desktop world, discussions regarding MAC vs. PC often occur with religious fervor. In the beginning, the accepted religion was that Apple had an advantage over the PC in terms of security. With the passage of time, the balance has shifted somewhat, especially as significant vulnerabilities have made the news.

OEMs may encounter religious issues when installing their software on a particular hardware platform. Some IT shops are all Dell, others exclusively IBM, and often they are willing to pay more to maintain that consistency, with the reason often being that it is simply easier. However, we have seen organizations undergo conversions, becoming more tolerant of alternative hardware "religions" upon learning that their platform of choice would cost an additional 15 percent.

Layer 10 – Economics

The final layer that is always a factor in a complete and compliant review, one way or another, is the operating budget. We're all familiar with examples. The executive who finally understands the full range of security and privacy requirements that bear on the business, and accepts the various changes that will be necessary to bring processes and systems into compliance, but then balks at the costs associated with full compliance. The IT manager who has ear-marked certain funds for a pet project and so sabotages the optimal business decision in favor of funding a sexier initiative.

It seems there is never enough budget to support full, proactive compliance. But money can always be found, somewhere, to repair compliance gaps when they become visible as the result of audits, security breaches, or worse. When those gaps occur, hindsight invariably tells us we should have spent the money on preventive measures, even if it was a larger investment than we had counted on. The results of compliance gaps can entail costs far beyond simple financial ones—although even those affect the bottom line eventually. Consider the impact of a worm or virus breaching your firewall and wreaking havoc in the user community, whether that consists of 20 employees or 20,000. Compare the cost of widespread employee downtime against the cost of the preventive measure that could have been implemented had an optimal purchase decision been made. Certainly, cost estimates may be and often are integrated into the purchase decision-making process in earlier layers. However, that doesn't preclude them from being considered later in a different light, such as the economic light cast in Layer 10.

Some security tests ask a question concerning the factor that has the most significant impact on security. Though you may be tempted to answer in terms of people, or policies, or some

technological barrier, this can be a trick question—for the impact of economics on final security decision-making may outweigh other factors.

Consider the \$3.8 billion multinational corporation that allocates \$10,000 per year on security. What is wrong with spending less than one one-hundredth of a percent to protect your organization's information assets? Plenty! Or, there's the publicly-traded New York firm with \$142 million in annual sales that spends \$450,000 per year on director and officer insurance, but only \$15,000 to prevent unauthorized network intrusion. These numbers do not compare favorably with the rule of thumb for IT investment, which is generally based on the number of company employee workstations multiplied by \$200 per month. And the security investment should be 10 percent of the IT budget.

Is it any wonder that U.S. businesses are under non-stop attack, that their security systems are being breached with ease, or that so-called private data about employees, clients, patients and customers is being stolen in broad cyber daylight?

There was a clever cartoon circulating in the IT community a few years ago in which a CFO sat behind a big desk, with an even bigger lighted sign mounted on the wall behind it. The sign flashed the word "No!" at the touch of a button. The CFO was sitting there anxiously awaiting his next visitor, so that he could have the satisfaction of flashing that big "No!" in answer to whatever funding they were requesting. Those organizations, and those CFOs, do exist—although the big lighted sign thankfully is pure metaphor. The more disturbing fact is that a request for funding may make complete sense for the organization, a business case may be well-constructed, and an expenditure may be perfectly timed to address a looming security need, but if there is no funding, none of that matters. This is Layer 10—abandon hope all who enter here!

Keeping systems updated with patches, especially the recent spate of system band-aids, requires considerable effort. Yet, too often, companies will not invest in the labor or technology resources needed to apply the patches and thereby avoid the risk of a security incident. Then, one day, an infected machine is plugged into the network and the infection spreads like wildfire. Suddenly, the famed knee-jerk scramble is in full swing. Thousands and thousands of dollars are spent freely to react to a crisis that could have been prevented—had the upfront investment been approved for labor and technology resources. One strategy for conquering a big "No!" obstacle like this is to tediously and relentlessly compile cost data until such a compelling, quantitative case for the expenditure is made that the CFO finds it increasingly difficult to refuse. Unfortunately, this takes time and persistence, but can ultimately pay off.

In South Florida, hurricanes are a fact of life—just as earthquakes are on the West Coast and tornados are in the Midwest. Yet there are companies who still refuse to pay for off-site hosting of critical servers and who have minimal battery-backup. In the South Florida example, several years had gone by without the experience of a direct threat, and many firms had begun to "play the odds." Unfortunately, when several storms did make landfall two years ago, some businesses were without power—and hence offline—for more than a week. Suddenly, the knee-jerk scramble was on, again. This time, IT VPs scrambled to locate a hosting facility anywhere, at any cost, transport their servers to the hosting facility, and try to get their systems up and running again. In the meantime, their web server and email servers were down and their websites dark. Customers had good reason to wonder if these businesses had simply blown away and weren't coming back.

Decisions to take calculated risks with network security programs can have similar consequences. For example, take the company that has a program in place, and decides that it provides an acceptable level of protection from unauthorized network intrusion. They go into deferred maintenance mode, saving money by avoiding upgrades and not investing in periodic audits of their systems and programs. When their system is hacked—as statistics indicate is more and more likely—customer data is compromised or stolen and the horse is out of the barn. Too late, they close the barn door. Too late, they invest in system protection. But now there are additional costs, and they are costs that easily could have been avoided:

- Compensating victims for damages due to identity theft
- Purchasing credit monitoring service for affected customers for a year or more
- Creating expensive advertising and direct mail campaigns to counter the enormous toll of negative publicity
- Attempting to recover lost business.

The very real examples make headlines almost every week—from retailers and grocery stores, to high schools and universities, to government agencies. From the fake subpoena scam targeting C-level executives to the viruses that are pre-installed on some of today's hot gadgets. The creativity and persistence of hackers, phishers and spammers seem to have no limits.

Lessons Learned

We have demonstrated the existence of three additional OSI layers in the information technology and security environment, which are often overlooked and undocumented. Real-life experiences have illustrated how those hidden layers can present obstacles to progress.

It is advantageous to be aware of all of the issues—including the non-technical—when developing a security project. This concept applies not just to hardware or programming, but to all project management. If political, religious or economic issues insert themselves into the mix, security architecture may be compromised and the opportunity to implement improved technology may be lost.

Although the political, religious and economic layers of the OSI model wield considerable power in influencing security decisions, they can be effectively managed. Following are some tips.

Don't ... be the IT Security Expert who enters the room with all the right answers, a 700-page audit report, and a long list of shortcomings that need fixing and fast. Executive management really isn't willing to change anything. (Remember, change is difficult, change consumes time, change requires investment.) IT Security Experts who stand their ground gain nothing. IT Security Experts who learn to leverage incremental progress—pushing for small changes a few at a time—ultimately will be much more effective in protecting their organizations.

Do ... your own due diligence when embarking on an IT security project. Are there relationships you should be aware of? Are there hardware, software or vendor biases you should be cognizant of? Is budget actually available? If not, what projects would have to be deferred in order to implement yours? Sometimes this type of research is as simple as asking for direction or guidance from an engaged executive. In other cases, conversations with colleagues who have been through similar experiences in attempting to effect change in their departments can

provide insights into the biases or preferences of the decision-making executives in your company.

Do ... initiate a dialog up your management chain to begin “warming up” your audience and pre-marketing your main ideas or premises. Provide preliminary information or a few samples of findings to garner feedback in the early stages. This will enable you to make adjustments in your project description, audit scope, or final recommendations that will improve your chances for success. Communication is a vital component at all stages of a project.

Do ... Begin building a solid business case for the security improvements that need to be made. Search the Internet for justification. The news is chock-full of detailed reports of identity theft, hacked systems, phishing scams, identity theft, hacked systems, phishing scams, identity theft, hacked systems, phishing scams—and the skyrocketing cost of these cybercrimes. Case studies can often be downloaded at no cost. Research is available from a variety of proven sources, and while the fully-detailed reports must be purchased, usually there are one or two compelling statistics or facts provided as part of the report marketing program. And don’t forget to tap your vendors or consultants for assistance as well.

Don’t ... become frustrated when the big “No!” sign keeps on flashing. To paraphrase the famous advice from Desiderata, “For all its sham, drudgery, and broken dreams, it is still a beautiful world. Be professional. Strive to be happy.”

Finally, if you are a C-level executive who ultimately makes the decisions regarding information security, ask yourself if you have been guilty of being stuck in one of these treacherous OSI layers. Have you ever rejected a good proposal for political, religious, or economic reasons? Did that action result in a sub-optimal decision—one that was not necessarily in the best interest of the company, that didn’t obtain all the bang for the buck it could have, or that eventually had to be re-thought in favor of a different course? We have all been guilty from time to time. The challenge is to keep an open mind, think outside the box, and try to make the right decisions for the right reasons. Empowering the talented professionals on your IT team to do their jobs is a good start.

Summary

Experience suggests, and strongly, that certain other factors affect information systems or security purchasing decisions, beyond the traditional seven layers of the OSI model. Most of us have seen evidence with our own eyes, whether as victims—such as the project team blindsided by the politics of a special vendor relationship—or as perpetrators, such as the executive team who has already made their decision but allows a process and recommendation to be completed for the record. It is important to understand these additional OSI layers and to be aware of the powerful influence they exert over information security decisions, even causing us to render sub-optimal decisions that are not in the best interests of our organizations. By considering the additional—and perhaps most influential—layers of the OSI model, CISOs, CIOs and IT professionals will afford themselves the best opportunity to make the right security decisions for the business, and thereby ensure optimal protection from malicious intrusion.

###

LIST OF REFERENCES

www.gartner.com

www.idc.com/research

Hannaford Data Breach: An Inside Job? Linda McGlasson, Bank Info Security Newsletter, April 22, 2008; www.bankinfosecurity.com/articles.php?art_id=835.

Phishing Scam Targets Corporate Execs; Stefanie Hoffman, ChannelWeb, April 16, 2008; www.crn.com/security/207400119?queryText=phishing+scam.

Can Technology Fix California Prison Health Care?; Kim Nash, CIO, April 11, 2008; www.cio.com/article/207150

FACT Act Identity Theft Red Flag Rules Alert; John Burnett, BankersOnline, April 2008; http://www.bankersonline.com/topstory/redflag_final.pdf

Consumer Alert: Phishing Attempts; Bank Info Security Agency Release, March 18, 2008; http://www.bankinfosecurity.com/regulations.php?reg_id=648.

Student Accused of Hacking School District Database; Joel Marino, South Florida Sun-Sentinel, March 15, 2008; www.topix.com/forum/source/south-florida-sun-sentinel/T6O00GB1EB8GBJVQ1.

Phishing Scams, Frivolous Arguments Top the 2008 "Dirty Dozen" Tax Scams; IRS-2008-41, March 13, 2008; www.irs.gov/newsroom/article/0,,id=180075,00.html.

Harvard Grad Students Hit in Computer Intrusion; Jaikumar Vijayan, Computerworld, March 13, 2008; www.infoworld.com/article/08/03/13/Harvard-grad-students-hit-in-computer-intrusion_1.html.

Some Viruses Come Pre-installed; Jordan Robertson, AP Technology Writer; March 13, 2008; www.newsvine.com/news/2008/03/13/1364485-some-viruses-come-pre-installed.

FBI: Cyber Crime Causes Financial Pain for Many Businesses; Keith Regan, E-Commerce Times, January 20, 2006; www.technewsworld.com/story/48417.html?welcome=1208986106.

Applying the OSI Seven-Layer Model to Information Security; Damon Reed, November 21, 2003; www.sans.org/reading_room/whitepapers/protocols/1309.php

www.ftc.gov/opa/2007

The author would like to extend special thanks to Terry Williams, Information Security Officer at City National Bank and former IT Security Technical Supervisor at Florida Power & Light Company, for his insightful contribution to the theoretical development of OSI Layers 8, 9 and 10.