AMCIS 2002 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2002

THE ORGANIZATIONAL INFORMATION INFRASTRUCTURE MATURITY MODEL: IMPLICATIONS FOR IT PROFESSIONALS

William Suchan
Arizona State University

The Organizational Information Infrastructure Maturity Model: Implications for IT Professionals

William K. Suchan
Arizona State University
will.suchan@asu.edu

Abstract

The ubiquity of computing is changing the face of information security and privacy, and information technology professionals must understand current trends in order to meet new challenges. In particular, those who develop the curricula used to educate IT professionals must ensure that the instruction is dynamic enough to keep pace not only with technology, but also with the unintended consequences of technological advances. This paper tracks the evolution of information technology professionals, and develops the need to focus effort towards the most vulnerable information systems. A new framework, the Organizational Information Infrastructure Maturity Model, is introduced. This model is designed to give organizations, especially non-infocentric organizations, the ability to assess the maturity of their information infrastructure. It simultaneously provides organizations with a roadmap for information process improvement. Ultimately, it will provide benchmarks for the education and certification of the next generation of IT professionals.

Introduction

Security and privacy are often considered to be mutually exclusive. While a strong argument can be made that this is true in a physical sense, in terms of personal information it can be argued that privacy is actually a subset of information security. Government agencies have spearheaded movements to make improvements in these areas. The Federal Trade Commission is the lead agency on privacy policy, while the National Security Agency oversees programs in information security.

While these efforts have resulted in marked improvement in information security and privacy in governmental organizations and large corporations, the amount of information that resides in smaller organizations continues to grow. These organizations, from small businesses to churches to local charitable organizations, don't always fall under the umbrella of the appropriate government agencies. In the past this was not a huge problem. Small organizations managed to fly under the radar. There were too many of them to allow for strict enforcement, and the limited amount of information that each organization controlled did not make them very vulnerable. This is changing, and the education of Information Technology (IT) professionals must change to address these growing vulnerabilities.

The IT Professional

The first generation of IT professionals was largely self-taught. When the first computer was installed for a business application in 1954 (Davis 1974), there were not any Computer Science or Management Information Systems programs in existence. The first generation of IT professionals was characterized by true pioneers who made revolutionary changes in the field (Glass 1998).

Over the next three decades the existing computer base grew exponentially, and university programs for IT professionals grew along with it. This growth led to the next generation of IT professionals – those who had the opportunity to receive a formal IT education before embarking into the field. This generation was characterized by many evolutionary changes in the discipline.

The explosive growth of the Internet and World Wide Web in the 1990's created an enormous demand for new solutions, as well as a new breed of IT professional. The latest generation is a mix of both self-taught pioneers and school-educated professionals. Together, they work to turn visions of a paperless and wireless infrastructure into reality. Even though information security is paramount, cutting edge innovations are unwittingly creating both less security and less privacy in a large number of information systems. A new generation of IT professionals must be educated so that technology-induced vulnerabilities can be addressed and overcome. To do this, a new infocentric paradigm for educating future IT professionals must be developed. Failure to do so will result in widespread loss of public confidence in the majority of existing information systems.

Existing Privacy Protection

A number of laws exist to ensure the privacy of personal information. The Federal Privacy Act of 1974, the Fair Credit Reporting Act, and the Family Educational Rights and Privacy Act, among others, were enacted to protect the private information of average citizens. Yet, it spite of these laws, the crime of identity theft is growing at an alarming rate. Part of the reason for this is that advances in technology are overwhelming provisions of existing law. As an example, the Fair Credit Reporting Act was initially established in 1970, and it was amended only four times in its first 20 years of existence. Since 1991 it has been amended at a rate of once a year (FTC 2002). Are IT professionals in the field staying abreast of these annual amendments? Are textbooks and lectures being updated annually for the benefit of students? While these are rhetorical questions, IT professionals and IT educators already know the unfortunate answers.

In 1999, the Graham-Leach-Bliley Act became law. This act addresses the disclosure of nonpublic personnel information and makes it illegal to fraudulently access financial information. The law recognizes the fact that financial institutions maintain sensitive information about individual citizens that can be misused in the hands of the wrong people. It puts controls on the way a financial institution may share information with affiliated companies. It also makes "pretexting" (obtaining personal information under false pretenses) a crime (FTC 2001). Unfortunately, making an activity illegal does not eliminate that activity. Activities such as pretexting can only be stopped by IT professionals who implement policies and procedures that make it harder for sensitive information to end up in the wrong hands.

Case Studies

While new laws have forced businesses to disclose their privacy policies, they have not necessarily increased privacy. The privacy disclosures simply act as a privacy interface between consumers and businesses. A comparison of the actual privacy disclosures of a major bank and a local car dealer (the companies involved will remain nameless) serve to highlight the differences in actual and perceived privacy protection afforded by the new laws.

A Major Bank

A major financial institution provides all customers with a copy of their privacy policy. It specifies in plain English not only what they do with information that they collect, but also who they share it with. In addition, the policy requires that affiliated companies must contractually agree to confidentiality and data protection provisions. Internally, this company has policies that require privacy and security training for employees. Additionally, the company restricts access to customer information to employees with a need to know, and password protects databases. Virus protection and intrusion detection software are used, and physical security of buildings is maintained. Audits are performed to ensure compliance, and the company maintains a dedicated privacy staff. A concerned consumer should feel comfortable that these measures will ensure the confidentiality of their personal information.

A Local Car Dealer

A local car dealership has each customer sign a privacy policy before dealing with any other paperwork in the car buying process. The form is written in standard legalese, and requires not one but two signatures. The first signature is to verify receipt of the policy. The second signature accompanies a box labeled "Opt Out". It appears that checking the box marked "Opt Out" box will prevent the dealer from sharing personal information with others. The next form that customers fill out is a credit application. This form is a multi-part form that produces a carbonless copy. The form asks for a plethora of personal information, to include bank account and credit card numbers and balances. It also requires phone number, birth date, Social Security Number, employer, salary, and other personal information. In short, it would give any unscrupulous individual everything they would need to steal an identity. In addition, it authorizes the dealer to perform a credit check. This not only verifies the data, but also lets any unscrupulous individual know if the subject is a worthwhile candidate for identity theft.

The privacy statement says that the dealer may collect nonpublic information from "consumers, customers, and former customers" and share that information with "affiliates or non-affiliated third parties." In essence, it says that they may collect information from anybody and share it with anybody. This complies with the law, since the policy is provided to customers, who acknowledge in writing that they received it. The cautious customer will be glad that they checked and signed the "Opt Out" box. Closer reading of the legalese reveals that even though the signed "Opt Out" designation was handed to the dealer, it doesn't go into effect unless the customer cuts off the "Opt Out" portion of the page and mails it to the dealer. Further investigation would reveal that the dealer may still share information with affiliated companies and financial institutions, as well as some non-affiliated third parties, even if the "Opt Out" form is properly returned by mail.

Vulnerable Information Systems

From a privacy standpoint, the car dealer case study is very chilling. Just because the dealer complies with the law doesn't mean that personal information is protected. The bank takes protection of personal information very seriously. It is able to protect information not by complying with the law, but by having a staff of IT professionals who implement systems and policies that facilitate information security. The car dealer has no IT staff. It has an information system that was installed by a "computer solution provider." Unlike the bank, the car dealer does not say what measures will be taken to ensure the security of customer information. Is information password protected, or does the stock boy have access? Worse yet, the personal data was collected on paper, and in duplicate. How will that paperwork be handled, stored, and disposed of?

Third generation IT professionals can develop effective schemes to secure the electronic information at the car dealership, but who is looking at the non-automated parts of the information system? People and paper are the weakest links in the system, and yet many IT professionals don't deal with anything that is not "high tech". The next generation of IT professionals needs to be educated as Information Professionals. In the past, *Information Technology* education was focused on *Technology*. In the future, IT education must focus on *Information*. Whether they are called Information Specialists, Information Engineers, or any other name, the next generation needs to be proficient in dealing with all forms of information.

Is the car dealer case study just an isolated example? While the slick wording of the privacy policy may remind one of the stereotypical used car salesman, the manner in which information is handled in this example is extremely common. Do any other types of organizations have similar business practices? These common practices include:

- Lack of a dedicated IT professional
- A locally procured/managed computer network
- A mixture of hard copy and electronic information
- The need to collect sensitive financial and personal information
- The ability to access credit reports/credit card numbers

In fact, many organizations fit this profile. A dentist's practice, an apartment manager, a real estate office, and a small furniture store all face privacy and security issues similar to those of the car dealer. Churches, political campaigns, and local non-profit organizations, who used to deal only with cash, now often deal with electronic payments, credit cards, and non-public information. Do any of these organizations have a dedicated information specialist? Typically not.

Great deals of time, effort, money, and research have gone into improvement of information security and privacy among government organizations and big businesses. Businesses of any size that engage in e-commerce are likewise greatly concerned about information security. In their recent book, Viega and McGraw (2001) provide guidelines for building secure software. The first item on their list is to secure the weakest link. In a macro sense, a piece of non-public information may exist simultaneously in many different systems. The "weakest link" for that piece of information is the system that is the least protected. A common thread amongst the types of organizations listed in the previous paragraph is that they are non-infocentric. As infocentric organizations continue to improve their cyber-security, non-infocentric organizations will increasingly become the weakest link in the information security chain. Criminals have always been a threat. In the 21st Century, another known worldwide threat is the international terrorist who steals identities or credit card numbers as a means of financing an operating cell. Why would a criminal or terrorist risk trying to break into a large bank to steal information when the same information is readily available at a church, car dealership, or real estate office?

The more thoroughly large information systems are protected, the more enticing small information systems will become. While the small systems are not as lucrative in terms of the amount of information that can be stolen at one time, the ease with which small systems can be targeted and the sheer number of small systems that exist (A national advertising campaign advises the public that over 90% of all businesses are small businesses.) make them high payoff targets. What percentage of useful information is stored in small systems? It is impossible to answer that question, but the answer is quite irrelevant. It really doesn't matter whether an identity or a credit card number is stolen from a bank or a church. Once stolen, the rightful owner will not know it is missing until it is too late.

The non-infocentric organization is truly the Achilles heel of global information systems. The community of Information Technology professionals needs to address the problem before it spins out of control. Just as well-publicized attacks on Internet-based businesses can cause a loss of consumer confidence, a well-publicized case of terrorists financing their operations by stealing information from a dentist or the heart association will forever change the way people view business.

The Organizational Information Infrastructure Maturity Model

Given the consequences of existing threats, wouldn't a person who owns or runs a non-infocentric organization take every possible action to prevent an information incident? Unfortunately, the answer is no. The problem is that most don't realize their vulnerability. Even if they did, many wouldn't know what to do about it. The International Information Systems Security Certification Consortium (ISC2 2002) has a program aimed at certifying information systems security professionals. While large organizations employ certified security professionals, small organizations simply cannot afford to hire a certified professional or to send their own employees for certification. A solution is needed that will bring the information security body of knowledge down to the realm of small organizations and thereby allow them to improve their information processes. The solution that I am proposing is the Organizational Information Infrastructure Maturity Model (OI2M2).

The model is patterned after successful maturity models that exist in other domains. In particular, I am modeling it after the original Capability Maturity Model defined by the Software Engineering Institute (SEI) at Carnegie Mellon University (Paulk et al. 1993). While numerous other maturity models have been developed in the last ten years, both within the SEI and by external organizations, the original model is simple enough to ensure usability by the target audience. A technical report about a more recent SEI model, the Capability Maturity Model Integration (Gallagher 2002, p. 22), says that "An enlightened leader within an operational organization could start a CMMI-based improvement program today without further model definition. Others may take these ideas and further refine them and propose an addition to the CMMI model framework that explicitly addresses operational needs." My proposal is to do just the opposite. I intend to develop the OI2M2 model to focus on improving information processes, but also to extend it by generalizing the model to serve a whole class of users (small, non-infocentric organizations) who do not otherwise have the wherewithal to tailor a model to their own needs.

Like the original SEI model, the OI2M2 can be used by organizations to assess their own vulnerabilities. Once vulnerabilities have been identified, the organization can use the model to guide themselves towards information process improvement. While assessment and improvement are certainly important, my larger purpose is to use the model as a change agent for information curricula. Key process areas for each level will be translated into information security curricular elements for various levels of students. Table 1 below shows how model levels correspond to educational levels.

Table 1. OI2M2 Level to Education Level Correlation

Level	Characteristic	Educational Level
1	Initial	
2	Repeatable	High School
3	Defined	2 year College / Continuing Education
4	Managed	2 year College / Continuing Education
5	Optimizing	4 year College / University

While there is not room here to describe the processes defined for each level of the model, the use of the model is far more critical than its eventual composition. Simply introducing infocentric education into high school computer and business classes will be an important first step. In time, the students who learn based on the curriculum derived from the model will be the employees of organizations using the model for self-assessment. This process will be accelerated by using students (at the college level) to assess outside organizations as part of their degree programs. The benefits of this are numerous. The students get real-world experience in dealing with an existing information system, the assessed organization gets outside eyes to look at its information processes, and the model gets to be evaluated for usefulness. This feedback loop is an important mechanism to ensure that the model remains current.

Realizing that those who go into certain high tech jobs will receive on-the-job training, another benefit of early education in information security is realized. As discussed by Bishop (2002, p. 32), students who are educated in security principles before receiving technical security training will require less training than their contemporaries. Additionally, they are more likely to finish training with a deeper understanding of concepts and will show more flexibility in application of their training. As more and more job positions interface with information and require security training, it will be a benefit for students to have an academic background in information security no matter what their intended field of study or profession.

Future Directions

Development of the OI2M2 model will continue over the next few years. Reported results from an IT Service model being developed in Amsterdam (Niessink and van Vliet 1999) give a good indication of the length of time that will be required before the model is fully populated. Their model is less than half done after more than two years of work. Because of the fluid nature of security and privacy, the OI2M2 will always be a work in progress. In parallel with model development, a working group is being formed to integrate the model into existing curricula. The working group includes educators from high schools and two and four year colleges. Additionally, leaders from business and government are being incorporated to assist in the validation of key process areas.

In 2004, the results of the first attempts at curriculum modification will be published. Additionally, the effects of the infocentric curriculum on students will be evaluated. The intent is twofold. First, the graduates entering the workforce should have greater information literacy. Second, more students are likely to continue their education in Information Technology if they are exposed to it at an earlier age. These efforts promise to lead more women and minorities into IT. It will take a few years to measure whether or not that actually happens. The ultimate goal is to have a self-sustaining organization that will shepherd the model and distribute the resulting infocentric curriculum modules.

Conclusion

Technology is being pushed to lower and lower levels, and the expertise to keep information secure is not being pushed down with it. As a result, information security is being reduced at the same time that it is being stressed throughout government and big business. A solution is needed to bring information security to organizations at all levels. The Organizational Information Infrastructure Maturity Model is one such solution. This is a tool that the next generation of information specialists can learn from in the classroom and take with them to the workplace. Once the model is well established, practitioners can be certified in its use, and organizations can have a way to let their customers know the extent of their commitment to ensuring customer privacy and the securing personal information.

References

Bishop, M. "Computer Security Education: Training, Scholarship, and Research," Security & Privacy supplement to IEEE Computer (35:4), 2002, pp. 30-32.

Davis, G. B. Management Information Systems: Conceptual Foundations, Structure, and Development. New York, New York: McGraw-Hill, 1974.

Federal Trade Commission (FTC) Website. "The Fair Credit Reporting Act," http://www.ftc.gov/os/statutes/fcrajan2002.pdf, 2002.

Federal Trade Commission (FTC) Website. "Gramm-Leach-Bliley Act – Financial Privacy and Pretexting," http://www.ftc.gov/privacy/glbact/index.html, 2001.

Gallagher, B.P. Interpreting Capability Maturity Model Integration for Operational Organizations. Pittsburgh, Pennsylvania: Software Engineering Institute, Carnegie Mellon University, 2002.

Glass, R. L. In the Beginning: Personal Recollections of Software Pioneers. Los Alamitos, California: IEEE Computer Society Press, 1998.

International Information Systems Security Certification Consortium, Inc. (ISC2) Website. “Certification,” http://www.isc2.org/cgi/content.cgi?category=3, 2002.

Niessink, F. and van Vliet, H. The Vrije Universiteit IT Service Capability Maturity Model. Amsterdam, The Netherlands: Vrije Universiteit Amsterdam, 1999.

Paulk, M. C., Curtis, B., Chrissis, M. B. and Weber, C. V. "Capability Maturity Model, Version 1.1," IEEE Software (10:4), 1993, pp. 18-27.

Viega, J., and McGraw, G. Building Secure Software: How to Avoid Security Problems the Right Way. Reading, Massachusetts: Addison-Wesley, 2001.