EMERGING ISSUES IN INFORMATION SECURITY MANAGEMENT

Taz Daughtrey
Editor-in-Chief
SOFTWARE QUALITY PROFESSIONAL
Lynchburg, VA 24502
Voice/Fax: 1 804 237 2723
SQP_Editor@asqnet.org

KEY WORDS

confidentiality, international standards, privacy

SUMMARY

Individuals and businesses are increasingly demanding accountability about the access and use of information provided with expectations of confidentiality (such as financial or medical data). Best-practice guidelines and international standards are now becoming available for specifying security requirements, for implementing appropriate controls, and for assessing and certifying compliance.

INTRODUCTION

New technologies invariably present new possibilities as well as new problems. Computing advances, especially coupled with communications advances as exemplified by the Internet, have facilitated an explosive growth in the speed and volume of information transactions. People are being asked to provide -- and to entrust to others whom they have never met – the most personal details of their preferences and purchases, of their financial and their physical health.

Faced with such demands, individuals are rightly concerned about how all that information will be protected and used. Businesses that rely on a steady flow of information confront a twofold dilemma: how to reassure customers that they can safely share personal information, and how to minimize their own risk that the data collected might be lost or compromised.

Security is therefore emerging as a significant quality requirement for information transactions. An "information economy" depends on the reliability of its lifeblood flow of information. Without confidence in that flow, the new technologies cannot provide their promised benefits.

What is meant by information security? ***Security*** can be thought of as protecting information from unauthorized access, alteration, or misuse. It is intertwined with the related concepts of ***privacy*** (controlling access to information as dictated by the owner or subject of the information) and ***confidentiality*** (the duty of custodian to prevent further disclosure of information or to release it only to the extent agreed upon). The interplay between these concerns has been illustrated in a commonplace scenario:

> If Mary Smith has a burglar alarm on her house, she has employed a *security* mechanism. When Mary decides to leave home for the weekend, she sets the alarm and activates security.
>
> When Mary asks Thelma next door (but not Jane down the street) to check on the pet hamster, she gives Thelma her burglar alarm security code. Mary has chosen to give access to Thelma. Mary has exercised her right to *privacy*.

> When Mary authorizes Thelma, and only Thelma, to enter her home, Mary trusts that Thelma will not bring someone else (such as Jane) inside Mary's home or give someone else the security code. The issue is one of *confidentiality*, trusting that Thelma will keep Mary's home off limits to others (PrivaComp 2001).
>
> .

The latest international standard on the subject (ISO/IEC 17799:2000) characterizes information security in terms of preserving *confidentiality*, *integrity*, and *availability*. The additional requirement for ***integrity*** is to ensure that data have not been undetectably altered or destroyed in an unauthorized manner, and ***availability*** addresses the concern that the data are accessible and useable upon demand by an authorized entity.

Others add the element of ***accountability*** to ensure that the actions of an entity can be traced, which in turn involves identification, authentication, and non-repudiation (evidence that will prevent a participant in an action from convincingly denying responsibility for the action and the integrity of its contents).

THE SITUATION

A few examples will illustrate the widespread and almost daily barrage of news about new security concerns.

> A recent study found credit card numbers and passwords stored on many "secure" Web servers are vulnerable to hacking. Eric Murray (2000), an independent security consultant and cryptology expert, tested a random sample of 8,081 secure Web servers and found that 32 percent of them are "dangerously weak."
>
> Health care officials point to an incident of alleged data theft at a leading cancer center in Boston as highlighting the security issues the industry faces. Moreover, security at health care organizations will come under increased scrutiny in coming months as federal agencies review regulations that require health organizations to protect the security and privacy of electronic information. (COMPUTERWORLD 2000)
>
> A fake news release – part of a stock-manipulation scheme -- about the electronics company Emulex within a few hours dropped its stock price by more than 60 percent, reducing its market capitalization by approximately $2.5 billion before trading was halted. (Allen 2000)

Vulnerabilities may be classed under the headings of disclosure, deception, disruption, and usurpation. Disclosure might result from acts of interception, inference, intrusion, or exposure. Deception could involve masquerade, falsification, or repudiation. Disruption includes incapacitation, corruption, and obstruction, while usurpation would be manifest as misappropriation or misuse. All in all, a daunting array of risks.

As Louise Kehoe (2001) has said, "Let's get real. The Internet will never be 100 per cent secure. Like most things in life, use of the Internet involves some risks and the best that anyone can hope for is to tilt the odds in favour of the "good guys" and away from those intent upon disruption.... Businesses that rely upon the Internet must come to terms with continuous security challenges and their associated costs, which may be substantial. Moreover, it is time to shed any pretence that the Internet can ever be immune to security risks."

There is a growing expectation that businesses will address these information security issues directly. One commercial "seal of approval" arrangement (Clicksure 2000) explicitly requires adherence to nine principles, three of which are in the realm of security.

Principle #4: **Privacy of Personal Information**
A Certified Internet Business must notify Users about its practices related to Personal Information it collects, holds, discloses or processes, and obtain and respect Users' choices regarding its use of their Personal Information.

Principle #5: **Confidentiality of Proprietary Information**
A Certified Internet Business must maintain the confidentiality of all Proprietary Information it collects, holds, discloses or processes.

Principle #6: **Information Security**
A Certified Internet Business must maintain systems to prevent any loss, misuse, or accidental or unauthorized access to or alteration of Users' Personal Information, Proprietary Information and payment details.

Interestingly, these principles have been placed on the same level as a further principle related to "quality."

Principle #8**: Demonstration of Quality**
Businesses must establish and demonstrate the effective implementation of appropriate quality management systems that cover their own activities and those provided by their suppliers and sub-contractors.

One might well perform information security management as parallel to, or even a subset of, quality management.

SOME INSIGHTS

Tradeoffs seem necessary to avoid extremes. Zero tolerance for risks such as fraud would put online merchants out of business. On the other hand, seeking perfect security would make a system useless. It is true that anything worth doing carries some risk. So what is an acceptable balance between safety and risk?

"[It is] a nightmare for any company hoping to offer both convenient access and secure data storage to its customers. Some would argue that this is fundamentally a zero-sum game -- that whatever one adds to make access more convenient will automatically subtract from security." (Register 2000)

A cost-of-security model may be considered analogous to the traditional cost-of-quality model. In this framework, the total cost for managing security is the sum of the costs expended for achieving security and the costs borne when security is not achieved. As with quality costs, one can categorize security achievement costs under the headings of ***prevention*** and ***appraisal***. Similarly, failing to achieve security may be manifest as ***internal failures*** or ***external failures***.

Typical *prevention* costs would be investment in procedure development, tools, and training; *appraisal* costs include audits and testing. *Failures* require rework, as well as loss of business and diminished reputation. A classic "pay me now or pay me later" situation applies here as elsewhere: "A small security review [appraisal] up front might cost $100,000, while an emergency response to an incident [failure] after the fact would run $350,000 to $500,000." (Lobel 2000)

Something as mundane as password management is actually one of the most labor-intensive and risk-prone IT functions, and costs between $200 and $300 per user each year (Gartner 2000). Yet the downside is that an organization's lack of proper password management could allow unauthorized access to, and misappropriation of, data valued potentially in the millions of dollars.

When the IT shop at Kaiser Permanente, the giant HMO based in Oakland, California, pumped information on hundreds of patients to the wrong people they did find the right way to handle a big privacy foul-up. "Human error created the problem, and a lot of hard human work was required to fix it…. Almost 900 patients had to be called. Regulators in 11 states had to be notified…. The patients seem to understand - the ones

whose privacy was violated and those whose mailboxes were flooded with other people's messages. Each one got a human voice explaining the problem. That alone went a long way to rebuild trust." (Hayes 2000) The primary cost here seems to have been in the rework, the effort that would not have been needed had the failure not occurred.

However, some losses are simply irretrievable. "The bank is insured; they can easily replace money lost in fraudulent transactions. What they can't give back is privacy." (Register 2000).

A considered approach to information security management might proceed through steps such as:

- Define information security policy.
- Define scope of management system.
- Assess risks: threats, vulnerabilities, impact.
- Manage risks: select suitable controls.
- Implement controls through procedures.
- Operate according to procedures. (BS 7799-2:1999)

RESPONSES

Over the past few years a number of international technical standards [ISO/IEC 9796, 9797, 9798, 9979, 10116, 10118, 11770, 13888, and 14888] have been adopted, addressing such security techniques as digital signatures, cryptography, and key management, as well as authentication and non-repudiation. More recently, framework documents have emerged to address a systematic way of planning to employ these technologies.

"Common Criteria for Information Technology Security Evaluation" (ISO/IEC 15408:1999) were adopted in 1999 and consist of

Part 1: Introduction and general model,
Part 2: Security functional requirements, and
Part 3: Security assurance requirements.

Part 1 provides the specification for the *Protection Profile* and the *Security Target* (or Target of Evaluation). The *Protection Profile* expresses the user's security needs in terms of both security functional requirements and security assurance requirements. The standard also provides pre-defined catalogs of these requirements. Part 2 provides a catalog of Security Functional Requirements, and Part 3 provides a catalog of Security Assurance Requirements. Part 3 further provides definitions of Evaluation Assurance Level (EALs), as follows:

EAL1 - functionally tested
EAL2 - structurally tested
EAL3 - methodically tested and checked
EAL4 - methodically designed, tested, and reviewed
EAL5 - semiformally designed and tested
EAL6 - semiformally verified design and tested
EAL7 - formally verified design and tested.

Contractual agreements specifying security requirements are thus able to reference an established definition of assurance level required for any evaluation.

December 1, 2000, marked the publication of the "Code of Practice for Information Security Management" (ISO/IEC 17799:2000). This consensus standard offers "recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings." Its content covers the range of security issues, addressed in the following sections:

- Organizational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management

- Access control
- Systems development and maintenance
- Business continuity management
- Compliance.

Analogies to broader quality management practices are striking. For instance, the standard recommends a security policy similar to the ISO 9001-mandated quality policy:

> Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

Further, the standard speaks to management review and internal audit:

> The security of information systems should be regularly reviewed.
> Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with security implementation standards (ISO/IEC 17799:2000).

A security policy might say (for a medical service provider):

> Our organization will not disclose personally identifiable patient information.
>
> Our organization will ensure that its workforce is trustworthy by certifying each employee through security training that addresses the commitments below.
>
> Employees will access confidential patient information only as necessary for performing assigned duties. No matter what the source, this information is not to be disclosed to others, except when authorized by the patient or required by law.
>
> Employees are to refrain from discussing or releasing confidential information about patients. All alleged, apparent, or potential breaches in patient confidentiality shall be reported to either the employee's immediate supervisor or the Chief Security Officer. All such reports are to be dispositioned by the Chief Security Officer.
>
> Each employee has the responsibility of reporting any violation of patient confidentiality brought to his or her attention.
>
> The Chief Security Officer performs ongoing audits for compliance to these policies and procedures.
>
> In accordance with the Employee Handbook, "unauthorized divulgence, removal, or copying of confidential information" may be cause for disciplinary action up to and including discharge. Other civil or criminal penalties may also be sought.

Where to start in implementing information security management? The "Code of Practice" enumerates controls either essential as legislative requirements or considered to be common best practice for information security. In the former category are those addressing:

- data protection and privacy of personal information;
- safeguarding of organizational records; and
- intellectual property rights.

Controls considered to be common best practice for information security include:

- information security policy document;
- allocation of information security responsibilities;
- information security education and training;
- reporting security incidents; and
- business continuity management (ISO/IEC 17799:2000).

Assurance activities are, in essence, a "confidence" game: the effort to provide *adequate confidence* that requirements – including security requirements -- are being met and that all stakeholders will be satisfied.

"Vendors of security products and services, and other interested parties, are predicting a surge of interest in the newly announced ISO 17799 information security code of practice." (Ovum 2001) BS 7799, on which ISO 17799 is based, has been used by thousands of organizations worldwide to review their security management practices, and several dozen in the UK have already gone on to obtain full BS7799 certification. The first North American registrations, interestingly, were mandated for the handling of TL9000 data under the supervision of the American Society for Quality.

One analyst claims, "When [17799] becomes better known as an international standard, companies worldwide will have to comply with it, because non-compliance will mean missing business opportunities. In the same way, not everybody has the ISO 9001 quality standard, but if you have it, people know you are following procedures which give the assurance of high [*sic*] quality of service. Some customers require business partners to be ISO 9001 certified." (Ovum 2001)

The British Standards Institution's own research indicates that a 100-person organization might need six person-days of auditing for compliance, at a cost of between $5000 and $8000, while 1,000 employees would take 25 auditor-days, at up to $33,000. Of course these appraisal costs need to be weighed against the direct failure cost of a security breach or that of the resulting loss of customers.

Wider certification is in everybody's interest. "Users should demand it from their suppliers; but it is also in their best interests to be compliant themselves, because they are less likely to suffer from security breaches, loss of data and so on. From the supplier's point of view, you can use the fact that you are compliant with [17799] as a marketing tool, either to win new customers or to enhance customer confidence in your business." (Ovum 2001)

Personnel certifications are also emerging. The International Information Systems Security Certifications Consortium [www.isc2.org] offers a designation of Certified Information Systems Security Professional, which measures knowledge about general security concepts. The SANS (System Administration, Networking, and Security) Institute [www.sans.org] sponsors individual certifications that focus on how to perform specific security tasks, for example, the Certified Intrusion Analyst recognition.

CONCLUSION

Attention is shifting from a narrow technical focus on the security of specific information transactions to a wider framework for creating business relationships with high levels of trust, based on confidence in business partners' systems and policies, including respect for individuals' confidentiality concerns.

Crucial success factors for information security management are recognized as:

- a security policy, objectives, and activities that reflect business objectives;
- an approach to implementing security that is consistent with the organizational culture;
- visible support and commitment from management;

- a good understanding of the security requirements, risk assessment, and risk management;
- effective marketing of security to all managers and employees;
- distribution of guidance on the security policy and standards to all employees and contractors;
- providing of appropriate training and education; and
- a comprehensive and balanced system of measurement used to evaluate performance in information security management and feed back suggestions for improvement (ISO/IEC 17799:2000).

The traditional software quality factors – functionality, reliability, usability, efficiency, maintainability, and portability – must now be joined by security.

Individuals cannot share personal information in good conscience, nor can businesses be assured of the integrity of their data-driven processes, without explicit specification and assurance of security requirements. "Trust me" is a valid model for interactions only where trust has been defined and demonstrated. If information transactions are to take full advantage of technological advances they must be grounded in well-established security management.

REFERENCES

Allen, C. 2000. "Fake News Release Costs Investors Millions." http://www.clickz.com/cgi-bin/gt/article.html?article=2345. September 5, 2000.

BS 7799-2:1999. Information Security Management -- Part 2: Specification for Information Security Management Systems. London: British Standards Institution.

Clicksure 2000. "The Confidence Standard for Electronic Business" Version 3.05. December 2000. Description at http://www.clicksure.com/hdiw-standard_index.htm

COMPUTERWORLD. 2000 "Health-Care Industry Looks at Security Risks.". http://www.idg.net/go.cgi?id=297150. August 14, 2000

Gartner Group report. 2000. Cited at http://www.informationweek.com/800/security.htm. August 21, 2000.

Hayes, F. 2000. "A Speedy Recovery." COMPUTERWORLD. http://www.computerworld.com/cwi/story/0,1199,NAV65-663_STO48797,00.html. August 21, 2000.

ISO/IEC 15408:1999. Common Criteria for Information Technology Security Evaluation. Geneva: International Organization for Standardization.

ISO/IEC 17799:2000. Code of Practice for Information Security Management. Geneva: International Organization for Standardization.

Kehoe, L. 2001. "Destroying the Internet Security Myth." FINANCIAL TIMES. February 1, 2001.

Lobel, M. 2000. http://www.informationweek.com/800/security.htm. August 21, 2000.

Murray, E. 2000. "SSL Server Security Survey." http://www.meer.net/~ericm/papers/ssl_servers.html. July 31, 2000.

Ovum. 2001. "Information security standard goes global - but not a lot of people know that." http://www.ovum.com/Articles/article.asp?file=019/global.htm. January 29, 2001.

PrivaComp. 2001. "Security, Privacy, and Confidentiality." http://www.patientfile.com/Security.htm

Register. 2000. "Barclay's failure" www.theregister.co. uk. August 3, 2000.