Achieving Privacy Through Security Measures

By C. Warren Axelrod, Ph.D., CISM, CISSP

The main difference between security and privacy is that, for privacy, the individual about whom the personal information is collected and handled effectively “owns” that information and, as such, should be able to control what happens to it. That is to say, the person should be able to control what personal information about him/her can be and is collected; ensure that it is correct and current; and decide who can look at it, share it and/or change it. However, there is considerable controversy over a recent change in AT&T’s privacy policy, whereby AT&T asserts that it collects information regarding customer access habits as they relate to AT&T Yahoo-branded web pages.1

The areas relating specifically to security or privacy and the intersection between information security and data privacy are shown in figure 1.

Functions that fall into the specific “information security only” space include physical security and human safety, business continuity planning, and disaster recovery planning. Factors falling into the “data privacy only” space include customer awareness via privacy notices, customer opt-in and opt-out options, and controls specific to customers who need to access, verify and modify personal information. Figure 2 indicates whether the various security categories, as listed in ISO 17799, relate to security, privacy or both.

The focus of this article is on examining security measures that impact privacy, namely the “common security/privacy factors” in figure 1. Areas and technologies that affect and are affected by privacy and security include access control, data protection and operational risk management, including incident response management.

Safeguarding Customer Information

In attachment A to the US Office of the Comptroller of the Currency (OCC) document OCC 2001-35 (available at www.ffiec.gov/exam/conference/Presentations/2001-35a.pdf), the OCC provides examination procedures for evaluating compliance with guidelines to safeguard customer information. The guidelines published by the OCC “…address standards for developing and implementing administrative, technical and physical safeguards to protect the security, confidentiality and integrity of customer information.” In the section of the OCC guidelines on evaluating the adequacy of risk management and control, the controls to be considered are shown in the left column of figure 3. Also shown are the specific security measures that can be used to establish and maintain the controls.

Controlling Application Access

The ability to monitor and control who can access what is paramount in the effort to protect personal information from unauthorized access and misuse. Applications are by far the preferred avenue of attack, as opposed to databases, since it is relatively easy for an outsider, and also insiders, to penetrate applications, since specialized knowledge of the infrastructure is not generally required. Consequently, it is of utmost importance to control access into applications and through them to functions, such as the ability to change or destroy the data. The exercise of protecting personal information from access via applications involves the management and control of access to the applications and ensuring that secure coding practices are enforced and tested.
Identity and Access Management (IAM)

IAM is unquestionably the most critical control for privacy and, in some ways, the most difficult and costly to implement. Users (sometimes included under the more general term “subjects”)—whether employees, customers, contractors or computer applications—are gaining authorized access to a rapidly increasing number of personal and corporate applications. The applications themselves are becoming more and more complex in terms of the permutations and combinations of potential services offered within each application and the interconnectivity among the applications. The growth in access rights is increasing exponentially as more capabilities are being introduced with the proliferation of applications, particularly those that are web-enabled. The advent of web services and service-oriented architecture (SOA) is calling into question the very definition of an application. The direction is toward the use of functions or services rather than traditional applications, and this will make the control of access much more difficult.

In addition to the burden of managing access, the privacy laws and regulations suggest, in effect, that details of use of personal information should be monitored and known at all times for every access or attempted access.2

Monitoring and controlling such a huge amount of activity creates enormously burdensome administrative overhead that can only be handled effectively, even in medium-sized organizations, through sophisticated automation. Unfortunately, such products have been slow in evolving and continue to lag behind the need for a universal product that is easy to implement and run in today’s complex computer and network worlds. Nevertheless, automation is generally the only feasible means of addressing the requirements for control, monitoring and response in the distributed systems and dispersed user environments.

<table>
<thead>
<tr>
<th>Risk Controls</th>
<th>Information Security Factors and Measures</th>
</tr>
</thead>
</table>
| Access controls, such as controls to authenticate and permit access to customers’ information by authorized persons only | • Identity and access management:  
  – Registration  
  – Authentication  
  – Authorization (entitlements)                                              |
| Encryption of electronically transmitted and stored customer data             | • Encryption policy and standards  
  • Provision of encryption technologies for all forms of end-to-end transmissions and all forms of storage media  
  • Strength of encryption warranted by risk related to specific circumstances |
| Procedures to ensure that system modifications are consistent with the approved security program | • Training in secure coding and security testing  
  • Security as part of the system development life cycle (SDLC)  
  • Application security reviews by third parties or internal staff |
| Monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, customer information systems | • Implementation of intrusion detection system (IDS) and intrusion prevention system (IPS) products  
  • Network and host monitoring and reporting systems  
  • Implementation of aggregation and correlation engines  
  • Reporting to include real-time alert systems  
  • Requirement for formal incident response and repair procedures |
| Dual control procedures, segregation of duties and employee background checks | • Regarding access administration, such as the review of access rights by owner of applications and/or data  
  • Regarding management of systems, restricted privileges (e.g., superuser) controlled by a different administrator from the one who is given privileged access |

Ensuring that the dictates of privacy laws and regulations are adhered to raises the bar on managing access to personal data. Legacy systems were never designed to provide the granularity needed to ensure compliance with today’s legal and regulatory requirements. To attain the necessary level of control and reporting for such systems, major changes need to be made to current legacy applications, or they need to be replaced. The costs of achieving this for the larger established organizations with core applications that are one, two or more decades old will typically run into the tens of millions of US dollars. To some extent, it is possible to front-end such systems with IAM products that offload many of the access administration functions previously handled by the applications themselves. However, this is still a considerable effort, as the intricacies of the controls within the applications have to be fully understood, and the applications must be amenable to such treatment.

Secure Coding, Testing and Change Management

Attacks on applications generally succeed because of vulnerabilities found in program code, less-secure settings in the utility software products and/or operating systems, or weaknesses in how the program has been implemented. Such discoveries might be accidental or might result from planned attacks. These vulnerabilities might lead to incursions into applications or systems, which in turn can result in unauthorized access to personal and other sensitive information.

There are many ways vulnerabilities can be avoided in custom-built applications and utilities and in commercial off-the-shelf (COTS) software. The most effective, and ultimately the least expensive, approach is to ensure that secure coding practices are included at every stage of the SDLC—in-house, at an outsourced software developer, or via a COTS software...
vendor. The design should be reviewed for conformance with secure design practices, and programmers and testers should be instructed as to appropriate techniques for making applications as secure as possible. Applications then need to be tested to ensure that the security standards have been implemented effectively. Individuals responsible for the infrastructure need to know the appropriate security baseline settings for operating systems, utilities, firewalls and the like. There should also be security assessments of the fully implemented systems, not only for the application, but also for the operating system and utilities that are required to run the applications—preferably conducted by an objective internal group or a reputable third party.

**Protecting the Data**

There are a number of ways in which data can be protected. The method most frequently touted, particularly by lawmakers who generally do not fully understand the technology, is encryption. But encryption does not protect against many hacking exploits and cracking programs, which are abundant and readily available over the Internet. Rather than encrypt, one might somehow disguise the data when used for testing purposes, so that, even when accessed, the scrambled data are useless. Finally, one must not forget that many data compromises are through “low tech” means, so that protection might encompass procedures for safeguarding physical media.

**Encryption**

Encryption is largely oversold and overrated as a technique for protecting personal information. In addition, its use can incur considerable costs in processing overhead and, where required, in the management of credentials and encryption keys.

Encryption generally originated from the needs of warfare, where the plans of the enemy were of tremendous value and the cost of encrypting was low relative to the value of the information being protected. Much of the value of encryption came from the difficulty and expense of otherwise protecting the information.

Today, encryption is commonly used to protect confidential and private information, generally when transmitted over networks. However, in the May 2001 issue of Information Security, Peter Tippett, then CTO of TruSecure (now Cybertrust), asserted, “The risk of having your credit card number sniffed on the public ‘Net is next to nothing.”

Less common is encrypting stored information, as it is more costly and difficult to implement. This is because the encrypting and decrypting of a transmitted message or an online session is generally a one-time event, meaning that the keys can be used once and do not have to be stored for future recovery purposes, as different keys can be created for each event without much operational impact. This is different from the encryption of stored data. Here there may be a frequent need to decrypt the data, meaning that the encryption keys have to be maintained over periods of time, often for more than a year, and a history of such keys must be maintained so that archived encrypted data can be retrieved and read. This represents a huge potential overhead cost of administration and maintenance. However, the value of encryption is also called into question when such methods as social engineering and insertion of malware (worms, Trojan horses, etc.) are cheaper and more effective in gaining access to “cleartext” data than attempting to decrypt the data.

The fallacy of certain laws, such as California (USA) SB 1386, is that legislators assume that encrypted data are well protected. It may be true that the data are protected from a direct hack against the database; however, it is much more likely that a successful attack will be through an application accessing the database, meaning that the compromised application will decrypt the data anyway. A common form of attack on customers’ financial applications is via “phishing,” where the customers’ credentials are hijacked so that access to accounts, and thus the data in those accounts, is not thwarted by encrypting the database. Key loggers—programs that are surreptitiously placed on a target’s PC to record selective keystrokes and transmit them to a third party—are also on the rise.

Nevertheless, encryption can be of some value, particularly if the assets protected are highly confidential or fit in the personal information category. It does make some types of attack more difficult and requires a hacker to take some positive action to determine what the data files contain through decryption. This is certainly more of a defense than keeping information such as passwords available in the clear, which can lead to easy identity theft.

Perhaps the main advantage that encryption provides is that it is somewhat of a deterrent and can avoid altogether certain types of break-ins. A casual user coming across an unencrypted file and seeing that it contains sensitive personal information might be tempted to use the information for bad purposes. That same user would likely not think (or would not be able) to decrypt it if it were an encrypted file, whereas someone with evil intent would certainly take advantage of such a fortuitous or intentional finding. As with many types of crime prevention measures, encryption might deter the amateur completely, but might only slow down the professional thief who is likely to have the break-in tools at hand.

**Protection Against Malware**

Malware includes computer viruses, worms, Trojan horses, denial of service (DoS) and spyware. Some of these nefarious programs are destructive or inhibiting, such as with many viruses, worms and DoS attacks. While these can be debilitating and costly to firms, they do not necessarily represent a direct threat to personal and confidential data. Much more insidious and risky in terms of disclosure of personal information are the viruses, worms and spyware (such as key loggers) intended to capture identity information from users or obtain personal and other confidential data directly.

Whereas, in the past, viruses were generally transmitted via infected removable media (such as floppy disks), the vast majority of viruses, worms and other malware now use the Internet as their main vector.

The usual protective measures for blocking viruses, worms and other destructive software include:

- Blocking e-mail attachments with specific extensions (such as .exe)
• Blocking e-mails for which the content is not allowed or is suspicious
• Denying access to certain web sites, such as those that might be used by worms or Trojan horses to receive directed data
• Monitoring network traffic and blocking suspicious source sites
• Blocking suspicious messages
• Applying current patches to remove vulnerabilities exploited by worms and other malware

While these measures do not guarantee that malware programs will not get into the internal network and systems, they go a long way in reducing the risk.

Data Disguise

Another vector for unintentionally disclosing personal and other confidential information is permitting unauthorized persons access to such data, either unwittingly or because it is not currently technically feasible to prevent it. While restricting such access is rightly handled through IAM products and procedures (as described previously), there may be limitations to these products because of how the applications have been written.

Nevertheless, if a user’s access to specific data fields cannot be restricted, there are products available that will scramble data into forms usable for testing, for example. This allows for the possibility of disguising certain components of a data file, such as personal information, so that those not authorized to access the data, particularly programmers and testers, can do their jobs without being shown personal and other sensitive data.

Handling of Data and Media

It is not sufficient to protect personal and other sensitive data while in transmission or when stored. The entire data life cycle must include protective measures—that is, the data must be protected during creation, transfer to a different custodian and disposal. Financial services regulators are increasingly paying attention to this area. In fact, the US Securities and Exchange Commission (SEC) recently published its final rules for disposing of consumer report information.6

What it all comes down to is that financial firms are being asked to implement protective measures on personal information at every stage in the process and for the length of time required for such data.

Operational Risk Management

Other methods for reducing the risk of inappropriate access, use and handling of personal data include monitoring and detection systems for catching misdeeds before they can take effect, thereby avoiding reportable incidents. However, in the event that bad things do happen, it is crucial to have effective response procedures and technologies in place to reduce the impact of a breach.

Monitoring and Detection Systems

Some laws and regulations require that companies report not only known successful attacks but also attempted attacks and attempts at unauthorized access and/or misuse. To be able to comply with such requirements, it is necessary to have in place tools and/or procedures that allow for the monitoring of the behavior of outsiders and valid users.

The best-known tools in this space are IDSs and access logging tools that can monitor and report on attempts at network intrusion and attacks against host computers. Such network-based and host-based products continuously monitor traffic over their respective components and alert operators to actual and potential unauthorized access.

There is another class of software or appliance product making inroads into the security marketplace, namely products that seek out anomalous behavior or detect unexpected occurrences of specific data items (such as Social Security numbers) among the streams of data traversing the internal networks and moving into or out of the enterprise network perimeter. Such products are designed to pick up unusual patterns that might suggest inappropriate or unlawful activities.

More advanced products are now offering the capability of not only detecting inappropriate accesses or anomalous behavior but also taking some action to stop such activities. These tools are known as IPSs. Their role is to match all activity against predetermined good and bad patterns and respond by intercepting and blocking bad behavior. While these tools can be very effective, they also present the danger of blocking valid traffic that might be caused by unusual, but acceptable, events and activities. For example, taking on or losing a large new customer might show up respectively as a valid surge or diminution in a particular type of traffic. The increase or reduction in traffic might activate the IPS and shut out important transactions. This can be overcome by programming the tool to accept anticipated transient behaviors. Of course, to be able to coordinate the expected traffic with the settings of the tools, it is necessary to have good communication between the business and technical areas.

Incident Avoidance, Response and Repair

A risk control that is often omitted from specific consideration of privacy relates to how to avoid incidents, even when an attack appears to have been successful, and how to respond to incidents, repair any damage done and make the changes necessary to avoid similar incidents in the future.

There are occasions on which it appears as though a breach has occurred, but actual activity resulting in unauthorized disclosure of personal information has not occurred. An example of this was an actual incident in which laptops containing unencrypted personal data belonging to a firm contracting to a financial services company were stolen. The financial services company activated the customer notification process as outlined in the “Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.”7 A short time later, the laptops were found and it was determined that the thief had not even powered up the laptops during the intervening period and was not aware that such information resided on the laptops. This raises the question as to when the customer notification mechanism should be activated. Regulators appear to be pushing for the proactive approach whereby customers are informed when there is a possibility that their personal
information has been compromised. This can lead to prematurely announcing an event that has not become a true incident. Clearly, had the data been encrypted, which was the policy of the institution, the situation would have been a non-event. What was needed here was a means of unequivocally enforcing the policy.

The manner in which actual incidents are handled, over and above the mandatory notification of customers, greatly affects the level of damage ultimately incurred. It is common to see systems become even more exposed following an incident, that is, during the review, repair and reconstruction phases. Those working on fixing the problem are often distracted from their regular duties because of the need to turn their attention to the recovery process. When that occurs, it is possible that other areas of vulnerability are neglected, thereby increasing the risk of further intrusions. It is important to lock down systems during this exposed period and pay particular attention to the logs from firewalls, IDSs and other monitors.

Conclusion

Complying with the burgeoning list of laws and regulations for protecting individuals’ personal information is not simple or straightforward given the inheritance of a multitude of computer systems that were built without comprehending the requirements for compliance that have recently evolved. Consequently, becoming compliant is turning out to require a major effort that will undoubtedly cost billions, if not tens or hundreds of billions, of US dollars, and require that a number of major structural and technical decisions will have to be made along the way. The expected expenditures on such efforts will far exceed what legislators, regulators and the private sector have anticipated, but the need to stem the tide of data breaches will largely override even the higher costs that evolve. Eventually, the pressure to update existing systems and ensure that new systems fully protect personal information at every step in its life cycle will prevail. The question will then become “Was it all worth it?” Many will think not.

Endnotes
2 While typical laws and regulations do not prescribe the specific technologies to use for compliance, the implications as to what needs to be done are readily apparent. However, it is usually left to organizations to justify their approach to complying with laws and regulations.
4 It should be noted that the e-mails used in phishing are not themselves considered malware (although newer versions have been noted as containing programs that scavenge for identity information), since they do not contain a dangerous payload. Instead, the e-mails use social engineering techniques to fool recipients into actively logging onto a fake web site.
6 Federal Register, vol. 68, no. 155, 12 August 2003, p. 47, 954-947, 960

Editor’s Note:

Outsourcing Information Security is available from the ISACA Bookstore. For information, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org, or telephone +1.847.253.1545, ext. 401 or 478. The book was reviewed in the Information Systems Control Journal, vol. 1, 2006.

C. Warren Axelrod, Ph.D., CISM, CISSP
is the business information security officer and chief privacy officer for United States Trust Company, N.A. At US Trust, he identifies, assesses and mitigates privacy and security risks and ensures that employees are familiar with privacy and security policy and procedures.

He is involved in the financial industry and at the national level with cybersecurity and critical infrastructure issues. He testified before the US Congress on cybersecurity in 2001. He was a founder and board member of the Financial Services Information Sharing and Analysis Center (FS/ISAC) and is a member of the Financial Services Sector Coordinating Council (FSSCC) Research and Development Committee.

He is the author of the book Outsourcing Information Security (Artech House, 2004), and his chapter on return on security investment will be included in Managing Information Assurance in Financial Services (Idea Group, 2007).