GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

The Bank Information Security Officer
Another Layer of Protection

GIAC Securities Essential Certification (GSEC) Practical Assignment
Version 1.4b – Option 1

Michele Lloyd
February 24, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

At one time, the bank security officer was the person who checked the alarms, and cameras, and brought employees into a room once a year and talked about bank holdup procedures. Now, although the currency in the vault must still be protected, the information about that money and its owners is as valuable as the currency itself. Protecting that information must be a main focus for the bank security professional. So much so that regulatory agencies considered requiring bank board of directors to designate a Corporate Security Officer to protect customer's information.[1]

Many financial institutions (and other organizations) have chosen to utilize managed security service providers (MSSPs) due to the challenges and costs they face to meet the ever-changing regulatory needs and the ever increasing threats and vulnerabilities. This discussion will focus on the in-house Information Security Officer, how that option can be a viable solution for a banking institution today, and how to integrate the Information Security Officer's role into a bank's comprehensive plan of defense in depth.

MSSPs[2]

When considering the magnitude of forces, tactics, code, and developed software available to be used to try and compromise the information that is being guarded, financial institutions and other companies may be easily drawn to the idea of the outsourced managed security service providers. Having fully trained, fully available, expert staff versed in all areas of information security is luxury that most institutions currently don't have. MSSPs can serve as a one-stop shop to implement best-practice solutions for perimeter protection of networks and firewalls, intrusion detection, risk assessment and other consulting needs. Because a qualified MSSP can spread costs of hardware, software and training over a number of clients, their services can be provided at less cost than an institution can absorb them. The MSSP can also provide an independent analysis of the company's entire security structure and compare that structure to other similar organizations.

This route is not without risks, however. Careful selection and negotiation must take place in the alignment with an MSSP to balance the total costs to the value

[1] Federal Reserve System, Federal Deposit Insurance Corporation. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule". 12 CFR Part 30, et al. 8630. URL: http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf. Page 16.

[2] Information from: Allen, Julia, et. al. "Outsourcing Managed Security Services", developed by Networked Systems Survivability Program at the Software Engineering Institute. Updated 01/21/03. URL: http://www.cert.org/security-improvement/modules/omss/b.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

of the services received in return. The MSSP has full-time dedicated professionals, but those services are spread amongst the number of organizations utilizing those services. The priorities of one organization may not be the priorities of the MSSP. Remedies and enhancements are dependent on the MSSP's allotment of resources to that organization. The relationship with an MSSP must be viewed the same as a relationship with any other service provider. Appropriate pre-approval review of the financial condition of the company, and proper receipt of service-level agreements are necessary steps in the selection of an MSSP. Consideration has to be made as to the business continuity risk if this provider for any reason is no longer available, or if the organization decides to terminate the services of that MSSP. An organization utilizing an MSSP must also continue to recognize and actively function with the understanding that the organization, along with the MSSP, ultimately bears the responsibility for the ownership and protection of the information. Any availability of the MSSP to the protected information also carries some degree of risk of compromise that must be evaluated.

With all these considerations, the decision to utilize a managed security service is not a forgone conclusion. The in-house Information Security Officer used in conjunction with a strong IT staff and a comprehensive committee structure can be an effective tool to providing a strategy of layers of defense.

Security Policy

The blueprint for an organization's security practices and procedures are the security policies. Correctly written, they serve as a comprehensive guideline upon which all security decisions can be based, and can provide staff with the responsibility and protection to implement that security. For a banking institution, written, board-approved policies are one of the mechanisms by which regulatory agencies examine their institutions. As an example, from the Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information (OCC 2001-35 Attachment A)[3], reviews of bank policies determine the bank's practices of risk assessment of systems and non-public information, the adequacy of the bank's program to manage and control those risks, and the controls exercised over information supplied to service providers.

An in-house Information Security Officer (ISO), with the integral knowledge of the institution, can provide valuable review and coordination of bank policies to ensure both regulatory compliance and effective security, along with assuring relevance to the goals of that institution. Review of the security policies can include:

1. Are written policies in place addressing administrative, technical and physical safeguards?

[3] Office of Comptroller of the Currency. "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information". OCC 2001-35. Attachment A. URL: http://www.ffiec.gov/exam/conference/Presentations/2001-35a.pdf 2-8.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2. Are the policies comprehensive and appropriate for that organization?
3. Do policies contain the required elements of purpose, clarity, relevance, viability, scope and ownership?
4. Are policies up-to-date and upgradeable?
5. Are multiple policies complementary, and are there any gaps in coverage?
6. Are policies written at various levels (program, system, issue, personal) as needed?
7. Are policies readily available and communicated throughout the organization?

Coordination of policies throughout an organization can be a challenging endeavor. The Information Security Officer with access and familiarity with various areas of the bank, can offer an objective viewpoint to combine and streamline appropriate policies into a cohesive plan. The"Y2K" plan developed in the 1990's, evolved into a Disaster Recovery Plan, can be transitioned into a Business Continuity Plan encompassing not only recovery from a physical threat, but also including losses of service providers and other risks, as well as recovery and assessment processes after an incident. Using the multitude of resources available, such as sample policies from The Sans Security Policy Project[4] meaningful policy statements can be developed.

Risk Assessment

The centerpiece of an organization's security policy is, of course, identification of what specifically is being secured. In traditional banking, protection of the currency from robbery was a clear-cut objective. The risk assessment process of a banking institution today is a multi-layered assessment of intertwining delivery channels, processes, and partnerships revolving around the customer's financial information. Since funds are transferred more and more without an exchange of currency, financial ownership of funds lies with whomever has the power to move those funds electronically between entities.

A risk analysis begins with a look at the customer information the bank or other organization possesses, with a ranking of that information. The more likely that information can be used in the movement of the funds between entities, the more critical the information is, and more securely it must be protected. All information obtained by the institution should be classified from most critical to least critical, with the understanding ANY customer information is not sharable to the public. Although a customer's name and address may be public knowledge in that it may be printed in a local phone directory, the fact that a bank has that information on file indicates some type of an ongoing relationship with them. Whether an individual or business is in fact a customer of that institution is privileged and caution must be exercised in the use of that information. Banks are also subject

[4] URL: http://www.sans.org/resources/policies/#template

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

to financial privacy requirements under the Gramm-Leach Bliley Act[5] to safeguard customer's "nonpublic personal information".

A sample categorization of protected assets may be:

1. High: Access codes, passwords, user rights, cash, monetary instruments and credit/debit cards.
2. Medium: Account information including account number, balance, and type of account, ownership information, and transaction history, as well as customer information such as social security number.
3. Low: Customer information including name, address, telephone number.

Once the information is classified, each individual delivery channel using this information to service the customer must be identified and assigned risk levels and tolerances. Such channels include over the counter delivery (tellers and customer service), telephone, ATM, point of sale, Internet, and through the necessary sharing of information with service providers.

In general, the over the counter delivery channels are protected via the establishment of internal controls, segregation of duties and are verified by the audit process. At the teller, customer service, and back-office levels, each functional area of the bank should be assigned factors based on various concerns such as credit risk, market risk, liquidity risk, operational risk, legal risk and reputation risk. Averaging these factors determines the frequency, and the extensiveness of the audit process. After each review, all findings and recommendations must be presented to the department, to senior management and to the board of directors. Responses and resolutions to the audit findings must be promptly tracked and verified.

Because of the electronic nature of bank delivery channels, each of those channels relies upon applications. Applications may be developed by the bank or purchased from a third party provider. Each individual application must be analyzed both before implementation, and on an on-going basis for risk. Each application should be evaluated under criteria such as the following:

1. Mission critical or non-critical?
2. Maintained in-house or outsourced?
3. Does it contain sensitive customer information?
4. Does the application process in a real-time or batch mode?
5. What are the threats and vulnerabilities?
6. What security is provided and utilized or can be developed?
7. What access/authentication methods are used?
8. What is the degree of effect of loss of service?

[5] Federal Trade Commission – Facts for Businesses. "In Brief: The Financial Privacy Requirements of the Gramm-Leach Bliley Act". URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

9. Is there accountability? Are all actions in the application traceable to their source?

Ongoing service-provider management is essential for all systems involving third parties. Once again, the level of management and the frequency of review is determined based on the above criteria. The initial review includes analysis of the financial condition of the provider, and negotiation of a signed contract containing a service-level agreement. Compliance with all current regulatory requirements must also be assured along with clarification on how regulatory changes will be implemented. The hardware and software requirements of any new application must be compatible with the existing network structure.

Surrounding and integrating the applications is an often-complex network structure. The importance and priority of protection of the network environment cannot be overstated, nor can the threats and potential for compromise. As Paul S. Raines, Federal Reserve Bank of New York's vice president of electronic security, states:

> I often joke that I am the only person at the Federal Reserve Bank of New York who can get fired because of the actions of a precocious 14-year-old script-kiddie. All kidding aside, security is such a complex issue with such a broad range of threats that it's difficult to demonstrate to stakeholders that every precaution has been taken to protect their digital assets. After all, even the very best information security managers armed with state-of-the-art systems can suffer a compromise.[6]

Fortunately, guidance for the bank ISO is available to arm themselves against the threats. The Federal Deposit Insurance Corporation provides detailed information for banks in the assessment and mitigation of these risks, and divides the task into the three functions of prevention, detection and response[7] with the risk assessment process as an element of prevention. Vulnerability assessment tools are one route to scan selected systems for potential compromise from known threats. Because these tools generally do not run on a continual basis, but are run in batch, that is, they take a snapshot of the system at the specific time, frequency and timing of scanning is a critical decision that must be made with the input of management. The Information Security Officer can serve as a liaison between network administrators and bank management, taking the administrator's assessment of tools for ease of use, efficiency of data extraction, database replenishment for new vulnerabilities and the reporting derived to Audit Committees and executive officers. Reporting from vulnerability scans should be able to be formatted so that that not only can the IT personnel decipher the

---

[6] Raines, Paul S. "Federal Reserve Bank / Image is everything. Protecting your organization's reputation is just as important as guarding your stake holder's assets". Information Security Magazine. November 2000. URL: http://infosecuritymag.techtarget.com/articles/november00/coverk.shtml

[7] Federal Deposit Insurance Corporation. "Risk Assessment Tools and Practices for Information System Security". FDIC's Financial Institution Letters. FIL9968a. Updated 07/17/99. URL: http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

output, but that the ISO can monitor results and relay them to management. Clear authority must be given when running any type of scanning, and the communication that scanning is occurring must be relayed appropriately to distinguish authorized assessment with unauthorized compromise attempts against the networks.

A combined risk portfolio of the bank's information, applications and networks must be assembled from the various assessments and then communicated to the board of directors on a regular frequency.

System Monitoring

Likewise, the Information Security Officer has an obligation in the ongoing practice of monitoring and detection of any violation of the bank's security. This should take many forms and include:

1. Awareness of the bank's network structure, including a basic understanding of the LAN and WAN topologies, servers, firewall and router placements, operating systems and any network segmentation.
2. Analysis of the physical security of the institution and systems containing critical information.
3. Verification of the optimization of configuration settings and various filtering techniques to provide the most protection, while at the same time providing for efficient use of the protected information for the bank's objectives. Changes to configuration settings must be logged and verified as authorized, appropriate, and then analyzed for any degradation of protection against vulnerabilities.
4. Assurance that protection exists at all stack layers of data transmission and that effective encryption of data is utilized where appropriate.
5. Assessment of intrusion detection system output information, and prompt research and reaction to any unusual activity.
6. Access control verification must take place at both the application and network levels. Are methodologies utilized to authorize new users appropriately with the least privileges needed to perform their jobs? Are job categories assigned with appropriate access and maintenance rights? Are authorization levels reviewed in conjunction with any employee's change in job function? Are effective password policies utilized? Is a comprehensive checklist utilized to deactivate all authority for terminated employees?
7. Utilization of penetration testing to assure the continued strength of security to outside forces.
8. Making sure virus protection software is utilized at multiple layers, and prompt and complete virus definition updates are performed.
9. Evaluation of potential scenarios and actual incidents to incorporate sound reaction plans, comprehensive documentation, and upgrading of policies and procedures accordingly.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

An appropriate summation of the monitoring responsibilities for a bank ISO is listed as an agenda item for an "Information Security and Fraud Prevention Telephone/Internet Training Session" by Bankers Systems, Inc. called "*Testing, training and tweaking"* [8]. Although this is listed in reference to deposit solutions, it is equally applicable to information security in general.

Even the most carefully constructed security plan cannot be assured to function properly without adequate testing in a situation that most closely resembles a production environment. If testing is properly done, and continues on a regular frequency, necessary "tweaking" of the security programs will result in order to maintain the desirable balance between confidentiality and integrity of information along with availability of the information to both the owners, and to the bank itself.

The monitoring process also lends itself to opportunities for training of the bank staff. Not only is formal training required on the bank's security policies, as well as expected practices of a system user, (password policies, internet usage, etc.) situations arise in the course of the process that allow for informal information sharing with employees. For example, Internet usage monitoring information can be used to explain how such usage can affect bandwidth, which in turn can cause detriment to the quality of communications on a phone system using IP telephony.

Reputation Protection

As Paul S. Raines of the Federal Reserve Bank of New York states:

> It may seem ludicrous to place reputation on par with the importance of data security, but it's a growing necessity in the age of lightning-fast media coverage and trigger-happy markets. Security breaches?even small ones?could lead customers, business partners and the general public to lose confidence in an organization.[9]

The traditionally loyal association banking customers had with their financial institution no longer exists. Instead of being the bank down the street with the tellers who know their names, a customer's association with a bank may rely solely via interaction with its online banking product. The quality and integrity of the information presented on the Internet, as well as the ability of the bank to convey the feeling that every practical, best-practice effort is being made to protect them may be the most important factor in that customer maintaining a banking relationship. Along with following all regulatory practices for Internet banking disclosures, a bank takes several steps to directly or indirectly portray to

[8] URL: http://www.bankerssystems.com/Bank/Deposit/html/fraud_prevention_telephone_training.htm

[9] Raines, Paul S. "Federal Reserve Bank / Image is everything. Protecting your organization's reputation is just as important as guarding your stake holder's assets". Information Security Magazine. November 2000. URL: http://infosecuritymag.techtarget.com/articles/november00/coverk.shtml

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the customers the level of commitment to privacy and security. Examples include:

1. A clearly expressed and prominently displayed privacy policy and security statement.
2. Detailed customer instructions regarding the steps the user is to take to guard their information.
3. Use of strong encryption methods, Secure Socket Layer and certificate based authentication.
4. Redundancy and strong backups for consistent availability of service.
5. Ownership assignment of bank web pages for constant monitoring against unauthorized modifications.

These points added onto the protections of the online banking system itself help to reinforce the trust relationship between the bank and customer.

Unfortunately, given the sheer number of potentials for attack, if the inevitable incident occurs, and (in a worst case scenario) results in some compromise of customer information, the bank's preparedness to assess the situation, to respond to and contain the attack, to minimize the loss, to assist the customer in the restoration of their assets, and to collect evidence for prosecution all demonstrate the bank's commitment to security and bolster the company's reputation.

Committee Structure

The advantages for an in-house Information Security Officer are the experience and knowledge of the organization's goals along with a vested interest in the success of that organization. These may be enhanced by a functioning committee structure. Joe Lockwood, First VP and Chief Technology Officer of COCC, describes one of eight steps for bank information security as communications supported by "Establishing a permanent security committee and drawing its members from all levels of the organization."[10] The sharing of ideas and perceptions of other employees to the bank's security program provides a more thorough review mechanism of all issues regarding security.

An organization of any size often has a number of committees where a component of its purpose deals with information and system security. By participation in various committee functions, a common thread of security awareness can be interjected throughout the groups.

If a technology committee looks at new advances that may be implemented in the delivery of banking products, a security analysis should be part of that

[10] Lockwood, Joe. "8 Steps to Securing Bank Information." URL: http://www.cocc.com/security.htm

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

consideration. A risk management committee may review any new product or service offered. The risk assessment process is one important responsibility of the ISO. An information steering committee may review specific updates and activities as well as initiatives undertaken by the IS department, many of which should be subject to review of the ISO. Likewise a vendor management committee may be formed to assess contracts with third party providers and maintain a system of review of those companies. The security element of information sharing with those entities is also subject to the ISO's consideration.

The Information Security Officer should be responsible to present any significant findings and periodic updates to the Audit Committee or to the Board of Directors as a whole.

Conclusion

"The FFIEC updates clearly establish information security as mission-critical for financial institutions, according to GartnerGroup analyst Richard De Lotto."[11] De Lotto continues by recommending monitoring, testing and the establishment of a formal security program in the accomplishment of this task. The in-house bank Information Security Officer working in conjunction with the Network Administrator, IT staff, and a strong committee structure, and with the support and allocation of resources by management can provide a valuable contribution to that end.

These combined resources can compare to qualifications of an outsourced provider, but can tailor security practices to the unique culture and goals of the individual institution. By the practices of policy creation and review, ongoing and multi-leveled risk analysis, careful implementation and review of sound security practices at all points of data transmission, efficient incidence response and by taking advantage of training opportunities, the ISO has a unique responsibility to the safety and security of the bank as well as to impart confidence and trust to its customers.

[11] As quoted in: Martin, Steven. "New Information Security Guidelines Issued". Bankers Systems & Technology Online. February 26, 2003. URL: http://www.banktech.com/story/whatsNews/BNK20030226S0007

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References:

- Federal Reserve System, Federal Deposit Insurance Corporation. "Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule". 12 CFR Part 30, et al. 8630. URL: http://www.ffiec.gov/exam/InfoBase/documents/02-joi-safeguard_customer_info_final_rule-010201.pdf. Page 16. (October 23, 2003)

- Information from: Allen, Julia, et. al. "Outsourcing Managed Security Services", developed by Networked Systems Survivability Program at the Software Engineering Institute. Updated 01/21/03. URL: http://www.cert.org/security-improvement/modules/omss/b.html (October 24, 2003)

- Office of Comptroller of the Currency. "Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information". OCC 2001-35. Attachment A. URL: http://www.ffiec.gov/exam/conference/Presentations/2001-35a.pdf 2-8. (October 24, 2003)

- URL: http://www.sans.org/resources/policies/#template. (October 23, 2003)

- Federal Trade Commission – Facts for Businesses. "In Brief: The Financial Privacy Requirements of the Gramm-Leach Bliley Act". URL: http://www.ftc.gov/bcp/conline/pubs/buspubs/glbshort.htm. (October 22, 2003)

- Raines, Paul S. "Federal Reserve Bank / Image is everything. Protecting your organization's reputation is just as important as guarding your stake holder's assets". Information Security Magazine. November 2000. URL: http://infosecuritymag.techtarget.com/articles/november00/coverk.shtml (October 23, 2003)

- Federal Deposit Insurance Corporation. "Risk Assessment Tools and Practices for Information System Security". FDIC's Financial Institution Letters. FIL9968a. Updated 07/17/99. URL: http://www.fdic.gov/news/news/financial/1999/FIL9968a.HTML. (October 23, 2003)

- URL: http://www.bankerssystems.com/Bank/Deposit/html/fraud_prevention_telephone_training.htm (October 22, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Lockwood, Joe. “8 Steps to Securing Bank Information.” URL: http://www.cocc.com/security.htm (October 23, 2003)

- Reymann, Paul. ”Information Technology and Security Officer Responsibilities”. BankersOnline.com. 03/11/02. URL: http://www.bankersonline.com/security/gurus_sec031102b.html. (October 23, 2003)

- As quoted in: Martin, Steven. “New Information Security Guidelines Issued”. Bankers Systems & Technology Online. February 26, 2003. URL: http://www.banktech.com/story/whatsNews/BNK20030226S0007 (October 24, 2003)

© SANS Institute 2004, Author retains full rights.