Incident Response Programs: Don't Get Caught Without One

Everyone is familiar with the old adage "Time is money." In the Information Age, data may be just as good. Reports of data compromises and security breaches at organizations ranging from universities and retail companies to financial institutions and government agencies provide evidence of the ingenuity of Internet hackers, criminal organizations, and dishonest insiders obtaining and profiting from sensitive customer information. Whether a network security breach compromising millions of credit card accounts or a lost computer tape containing names, addresses, and Social Security numbers of thousands of individuals, a security incident can damage corporate reputations, cause financial losses, and enable identity theft.

Banks are increasingly becoming prime targets for attack because they hold valuable data that, when compromised, may lead to identity theft and financial loss. This environment places significant demands on a bank's information security program to identify and prevent vulnerabilities that could result in successful attacks on sensitive customer information held by the bank. The rapid adoption of the Internet as a delivery channel for electronic commerce coupled with prevalent and highly publicized vulnerabilities in popular hardware and software have presented serious security challenges to the banking industry. In this high-risk environment, it is very likely that a bank will, at some point, need to respond to security incidents affecting its customers.

To mitigate the negative effects of security breaches, organizations are finding it necessary to develop formal incident response programs (IRPs).[1] However, at a time when organizations need to be most prepared, many banks are finding it challenging to assemble an IRP that not only meets minimum requirements (as prescribed by Federal bank regulators), but also provides for an effective methodology to manage security incidents for the benefit of the bank and its customers. In response to these challenges, this article highlights the importance of IRPs to a bank's information security program and provides information on required content and best practices banks may consider when developing effective response programs.

The Importance of an Incident Response Program

A bank's ability to respond to security incidents in a planned and coordinated fashion is important to the success of its information security program. While IRPs are important for many reasons, three are highlighted in this article.

First, though incident prevention is important, focusing solely on prevention may not be enough to insulate a bank from the effects of a security breach. Despite the industry's efforts at identifying and correcting security vulnerabilities, every bank is susceptible to weaknesses such as improperly configured systems, software vulnerabilities, and zero-day exploits.[2] Compounding the problem is the difficulty an organization experiences in sustaining a "fully secured" posture. Over the long term, a large amount of resources (time, money, personnel, and expertise) is needed to maintain security commensurate with all potential vulnerabilities. Inevitably, an organization faces a point of diminishing returns whereby the extra resources

[1] In its simplest form, an IRP is an organized approach to addressing and managing the aftermath of a security breach or attack.

[2] A zero-day exploit is one that takes advantage of a security vulnerability on the same day that the vulnerability becomes generally known.

applied to incident prevention bring a lesser amount of security value. Even the best information security program may not identify every vulnerability and prevent every incident, so banks are best served by incorporating formal incident response planning to complement strong prevention measures. In the event management's efforts do not prevent all security incidents (for whatever reason), IRPs are necessary to reduce the sustained damage to the bank.

Second, regulatory agencies have recognized the value of IRPs and have mandated that certain incident response requirements be included in a bank's information security program. In March 2001, the FDIC, the Office of the Comptroller of the Currency (OCC), the Office of Thrift Supervision (OTS), and the Board of Governors of the Federal Reserve System (FRB) (collectively, the Federal bank regulatory agencies) jointly issued guidelines establishing standards for safeguarding customer information, as required by the Gramm-Leach-Bliley Act of 1999.[3] These standards require banks to adopt response programs as a security measure. In April 2005, the Federal bank regulatory agencies issued interpretive guidance regarding response programs.[4] This additional guidance describes IRPs and prescribes standard procedures that should be included in IRPs. In addition to Federal regulation in this area, at least 32 states have passed laws requiring that individuals be notified of a breach in the security of computerized personal information.[5] Therefore, the increased regulatory attention devoted to incident response has made the development of IRPs a legal necessity.

Finally, IRPs are in the best interests of the bank. A well-developed IRP that is integrated into an overall information security program strengthens the institution in a variety of ways. Perhaps most important, IRPs help the bank contain the damage resulting from a security breach and lessen its downstream effect. Timely and decisive action can also limit the harm to the bank's reputation, reduce negative publicity, and help the bank identify and remedy the underlying causes of the security incident so that mistakes are not destined to be repeated.

Elements of an Incident Response Program

Although the specific content of an IRP will differ among financial institutions, each IRP should revolve around the minimum procedural requirements prescribed by the Federal bank regulatory agencies. Beyond this fundamental content, however, strong financial institution management teams also incorporate industry best practices to further refine and enhance their IRP. In general, the overall comprehensiveness of an IRP should be commensurate with an institution's administrative, technical, and organizational complexity.

Minimum Requirements

The minimum required procedures addressed in the April 2005 interpretive guidance can be categorized into two

[3] Appendix B to Part 364 of the FDIC Rules and Regulations at www.fdic.gov/regulations/laws/rules/2000-8660.html#2000appendixbtopart364 and FDIC FIL-22-2001, Guidelines Establishing Standards for Safeguarding Customer Information, issued March 14, 2001. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); and 12 CFR 570, App. B (OTS).

[4] FDIC FIL-27-2005, Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, issued April 1, 2005, www.fdic.gov/news/news/financial/2005/fil2705.html. Also refer to 12 CFR 30, App. B (OCC); 12 CFR 208, App. D-2 and 12 CFR 225, App. F (FRB); 12 CFR 364, App. B (FDIC); and 12 CFR 570, App. B (OTS).

[5] "State Security Breach Notification Laws (as of June 2006)," September 15, 2006, www.thecyberangel.com/StSecBrchNotifLaw.doc.

Incident Response Programs

continued from pg. 5

broad areas: "reaction" and "notification." In general, reaction procedures are the initial actions taken once a compromise has been identified. Notification procedures are relatively straightforward and involve communicating the details or events of the incident to interested parties; however, they may also involve some reporting requirements. Figure 1 lists the minimum required procedures of an IRP as discussed in the April 2005 interpretive guidance.

Reaction Procedures

Assessing security incidents and identifying the unauthorized access to or misuse of customer information essentially involve organizing and developing a documented risk assessment process for determining the nature and scope of the security event. The goal is to efficiently determine the scope and magnitude of the security incident and identify whether customer information has been compromised.

Containing and controlling the security incident involves preventing any further access to or misuse of customer information or customer information systems. As there are a variety of potential threats to customer information, organizations should anticipate the ones that are more likely to occur and develop response and containment procedures commensurate with the likelihood of and the potential damage from such threats. An institution's information security risk assessment can be useful in identifying some of these potential threats. The containment procedures developed should focus on responding to and minimizing potential damage from the threats identified. Not every incident can be anticipated, but institutions should at least develop containment procedures for reasonably foreseeable incidents.

Notification Procedures

An institution should notify its primary Federal regulator as soon as it becomes aware of the unauthorized access to or misuse of sensitive customer information or customer information systems. Notifying the regulatory agency will help it determine the potential for broader ramifications of the incident, especially if the incident involves a service provider, as well as assess the effectiveness of the institution's IRP.

Institutions should develop procedures for notifying law enforcement agencies and filing SARs in accordance with their primary Federal regulator's requirements.[6] Law enforcement agencies may serve as an additional resource in handling and documenting the incident. Institutions should also establish procedures for filing SARs in a timely manner

Figure 1

Minimum Requirements

Develop reaction procedures for	Establish notification procedures for
assessing security incidents that have occurred;	the institution's primary Federal regulator;
identifying the customer information and information systems that have been accessed or misused; and	appropriate law enforcement agencies (and filing Suspicious Activity Reports [SARs], if necessary); and
containing and controlling the security incident.	affected customers.

[6] An institution's obligation to file a SAR is specified in the regulations of its primary Federal regulator. Refer to 12 CFR 21.11 (OCC), 12 CFR 208.62 (FRB), 12 CFR 353 (FDIC), and 12 CFR 563.180 (OTS).

because regulations impose relatively quick filing deadlines. The SAR form[7] itself may serve as a resource in the reporting process, as it contains specific instructions and thresholds for when to file a report. The SAR form instructions also clarify what constitutes a "computer intrusion" for filing purposes. Defining procedures for notifying law enforcement agencies and filing SARs can streamline these notification and reporting requirements.

Institutions should also address customer notification procedures in their IRP. When an institution becomes aware of an incident involving unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to determine the likelihood that such information has been or will be misused. If the institution determines that sensitive customer information has been misused or that misuse of such information is reasonably possible, it should notify the affected customer(s) as soon as possible. Developing standardized procedures for notifying customers will assist in making timely and thorough notification. As a resource in developing these procedures, institutions should reference the April 2005 interpretive guidance, which specifically addresses when customer notification is necessary, the recommended content of the notification, and the acceptable forms of notification.

Best Practices—Going Beyond the Minimum

Each bank has the opportunity to go beyond the minimum requirements and incorporate industry best practices into its IRP. As each bank tailors its IRP to match its administrative, technical, and organizational complexity, it may find some of the following best practices relevant to its operating environment. The practices addressed below are not all inclusive, nor are they regulatory requirements. Rather, they are representative of some of the more effective practices and procedures some institutions have implemented. For organizational purposes, the best practices have been categorized into the various stages of incident response: preparation, detection, containment, recovery, and follow-up.

Preparation

Preparing for a potential security compromise of customer information is a proactive risk management practice. The overall effectiveness and efficiency of an organization's response is related to how well it has organized and prepared for potential incidents. Two of the more effective practices noted in many IRPs are addressed below.

Establish an incident response team.

A key practice in preparing for a potential incident is establishing a team that is specifically responsible for responding to security incidents. Organizing a team that includes individuals from various departments or functions of the bank (such as operations, networking, lending, human resources, accounting, marketing, and audit) may better position the bank to respond to a given incident. Once the team is established, members can be assigned roles and responsibilities to ensure incident handling and reporting is comprehensive and efficient. A common responsibility that banks have assigned to the incident response team is developing a notification or call list, which includes contact information for employees, vendors, service providers, law enforcement, bank regulators, insurance companies, and other appropriate contacts. A comprehensive notification list can serve as a valuable resource when responding to an incident.

[7] See www.fincen.gov/reg_bsaforms.html.

Incident Response Programs

continued from pg. 7

Define what constitutes an incident.

An initial step in the development of a response program is to define what constitutes an incident. This step is important as it sharpens the organization's focus and delineates the types of events that would trigger the use of the IRP. Moreover, identifying potential security incidents can also make the possible threats seem more tangible, and thus better enable organizations to design specific incident-handling procedures for each identified threat.

Detection

The ability to detect that an incident is occurring or has occurred is an important component of the incident response process. This is considerably more important with respect to technical threats, since these can be more difficult to identify without the proper technical solutions in place. If an institution is not positioned to quickly identify incidents, the overall effectiveness of the IRP may be affected.[8] Following are two detection-related best practices included in some institutions' IRPs.

Identify indicators of unauthorized system access.

Most banks implement some form of technical solution, such as an intrusion detection system or a firewall, to assist in the identification of unauthorized system access. Activity reports from these and other technical solutions (such as network and application security reports) serve as inputs for the monitoring process and for the IRP in general. Identifying potential indicators of unauthorized system access within these activity or security reports can assist in the detection process.

Involve legal counsel.

Because many states have enacted laws governing notification requirements for customer information security compromises, institutions have found it prudent to involve the institution's legal counsel when a compromise of customer information has been detected. Legal guidance may also be warranted in properly documenting and handling the incident.

Containment

During the containment phase, the institution should generally implement its predefined procedures for responding to the specific incident (note that containment procedures are a required minimum component). Additional containment-related procedures some banks have successfully incorporated into their IRPs are discussed below.

Establish notification escalation procedures.

If senior management is not already part of the incident response team, banks may want to consider developing procedures for notifying these individuals when the situation warrants. Providing the appropriate executive staff

[8] Pursuant to section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), the FDIC, the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Office of Thrift Supervision, the National Credit Union Administration, and the Federal Trade Commission, have jointly proposed (1) guidelines for financial institutions and creditors identifying patterns, practices, and specific forms of activity, that indicate the possible existence of identity theft, and (2) regulations requiring each financial institution and creditor to establish reasonable policies and procedures for implementing the guidelines. The notice of proposed rulemaking (NPR) also includes provisions requiring credit and debit card issuers to assess the validity of a request for a change of address under certain circumstances, and, pursuant to section 315 of the FACT Act, guidance regarding reasonable policies and procedures that a user of consumer reports must employ when such a user receives a notice of address discrepancy from a consumer reporting agency. The NPR was published on July 18, 2006, at 71 Fed. Reg. 40786, and the comment period ended on September 18, 2006. The agencies are reviewing the comments received in preparation for a final rule.

and senior department managers with information about how containment actions will affect business operations or systems and including these individuals in the decision-making process can help minimize undesirable business disruptions. Institutions that have experienced incidents have generally found that the management escalation process (and resultant communication flow) was not only beneficial during the containment phase, but also proved valuable during the later phases of the incident response process.

Document details, conversations, and actions.

Retaining documentation is an important component of the incident response process. Documentation can come in a variety of forms, including technical reports generated, actions taken, costs incurred, notifications provided, and conversations held. This information may be useful to external consultants and law enforcement for investigative and legal purposes, as well as to senior management for filing potential insurance claims and for preparing an executive summary of the events for the board of directors or shareholders. In addition, documentation can assist management in responding to questions from its primary Federal regulator. It may be helpful during the incident response process to centralize this documentation for organizational purposes.

Organize a public relations program.

Whether a bank is a local, national, or global firm, negative publicity about a security compromise is a distinct possibility. To address potential reputation risks associated with a given incident, some banks have organized public relations programs and designated specific points of contact to oversee the program. A well-defined public relations program can provide a specific avenue for open communications with both the media and the institution's customers.

Recovery

Recovering from an incident essentially involves restoring systems to a known good state or returning processes and procedures to a functional state. Some banks have incorporated the following best practices related to the recovery process in their IRPs.

Determine whether configurations or processes should be changed.

If an institution is the subject of a security compromise, the goals in the recovery process are to eliminate the cause of the incident and ensure that the possibility of a repeat event is minimized. A key component of this process is determining whether system configurations or other processes should be changed. In the case of technical compromises, such as a successful network intrusion, the IRP can prompt management to update or modify system configurations to help prevent further incidents. Part of this process may include implementing an effective, ongoing patch management program, which can reduce exposure to identified technical vulnerabilities. In terms of non-technical compromises, the IRP can direct management to review operational procedures or processes and implement changes designed to prevent a repeat incident.

Test affected systems or procedures prior to implementation.

Testing is an important function in the incident response process. It helps ensure that reconfigured systems, updated procedures, or new technologies implemented in response to an incident are fully effective and performing as expected. Testing can also identify whether any adjustments are necessary prior to implementing the updated system, process, or procedure.

Incident Response Programs

continued from pg. 9

Follow-up

During the follow-up process, an institution has the opportunity to regroup after the incident and strengthen its control structure by learning from the incident. A number of institutions have included the following best practice in their IRPs.

Conduct a "lessons-learned" meeting.

Successful organizations can use the incident and build from the experience. Organizations can use a lessons-learned meeting to

- discuss whether affected controls or procedures need to be strengthened beyond what was implemented during the recovery phase;
- discuss whether significant problems were encountered during the incident response process and how they can be addressed;
- determine if updated written policies or procedures are needed for the customer information security risk assessment and information security program;
- determine if updated training is necessary regarding any new procedures or updated policies that have been implemented; and
- determine if the bank needs additional personnel or technical resources to be better prepared going forward.

The preceding best practices focused on the more common criteria that have been noted in actual IRPs, but some banks have developed other effective incident response practices. Examples of these additional practices are listed in Figure 2. Organizations may want to review these practices and determine if any would add value to their IRPs given their operating environments.

What the Future Holds

In addition to meeting regulatory requirements and addressing applicable industry best practices, several characteristics tend to differentiate banks. The most successful banks will find a way to integrate incident response planning into

Figure 2

Additional IRP Best Practices

Test the incident response plan (via walk-through or tabletop exercises) to assess thoroughness.

Implement notices on login screens for customer information systems to establish a basis for disciplinary or legal action.

Develop an incident grading system that quantifies the severity of the incident, helps determine if the incident response plan needs to be activated, and specifies the extent of notification escalation.

Provide periodic staff awareness training on recognizing potential indicators of unauthorized activity and reporting the incident through proper channels. Some institutions have established phone numbers and e-mail distribution lists for reporting possible incidents.

Inform users about the status of any compromised system they may be using.

Establish a list of possible consultants, in case the bank does not have the expertise to handle or investigate the specific incident (especially regarding technical compromises).

Establish evidence-gathering and handling procedures aimed at preserving evidence of the incident and aiding in prosecution activities.

normal operations and business processes. Assimilation efforts may include expanding security awareness and training initiatives to reinforce incident response actions, revising business continuity plans to incorporate security incident responses, and implementing additional security monitoring systems and procedures to provide timely incident notification. Ultimately, the adequacy of a bank's IRP reflects on the condition of the information security program along with management's willingness and ability to manage information technology risks. In essence, incident response planning is a management process, the comprehensiveness and success of which provide insight into the quality and attentiveness of management. In this respect, the condition of a bank's IRP, and the results of examiner review of the incident response planning process, fit well within the objectives of the information technology examination as described in the Information Technology–Risk Management Program.[9]

An IRP is a critical component of a well-formed and effective information security program and has the potential to provide tangible value and benefit to a bank. Similar to the importance of a business continuity planning program as it relates to the threat of natural and man-made disasters, sound IRPs will be necessary to combat new and existing data security threats facing the banking community. Given the high value placed on the confidential customer information held within the financial services industry, coupled with the publicized success of known compromises, one can reasonably assume that criminals will continue to probe an organization's defenses in search of weak points. The need for response programs is real and has been recognized as such by not only state and Federal regulatory agencies (through passage of a variety of legal requirements), but by the banking industry itself. The challenges each bank faces are to develop a reasonable IRP providing protections for the bank *and* the consumer and to incorporate the IRP into a comprehensive, enterprise-wide information security program. The most successful banks will exceed regulatory requirements to leverage the IRP for business advantages and, in turn, improved protection for the banking industry as a whole.

Eric R. Morris
Information Technology Examiner, Chicago, IL

John J. Sosnowski II
Examiner, Indianapolis, IN

[9] The Information Technology–Risk Management Program (IT–RMP) is the approach for conducting information technology examinations at FDIC-supervised institutions, regardless of size and complexity. FIL 81-2005, Information Technology–Risk Management Program New Information Technology Examination Procedures, August 18, 2005, www.fdic.gov/news/news/financial/2005/fil8105.html.