



By
Doug
Johnson

INTO THE

Bankers, congratulations—you have made the big screen! *Firewall*, starring Harrison Ford, opened in theaters in February.

In the film, computer security specialist Jack Stanfield works for the Seattle-based Landrock Pacific Bank. A trusted top-ranking executive, he has built his career and reputation on designing the most effective antitheft computer systems in the industry, protecting the bank's financial holdings from the constant threat of increasingly sophisticated hackers with his complex network of tracers, access codes, and firewalls.

But there's a hidden vulnerability in the system he didn't account for—himself.

Our hero gets hacked. The bad guys monitor his activities, including his Internet banking account, and get personal information that enables them to kidnap his kids. So our friend Jack is supposed to steal millions of dollars electronically from his own bank to get his kids back.

While this movie has been kicking around since 2004, it is not surprising that it made it into production, considering that we just experienced what the *Washington Post* termed “the year of the security breach.” I don't know about you, but I could stand to be a little less popular.

Breaches Happen

The bottom line is that while bankers “get” information security and the vital importance of safeguarding customer information, many portions of the business and even government communities with which we do business have been involved in the recent data breaches affecting our customers:

- Retailers have had their computer systems breached

while keeping customer transactional data that should not have been stored after the transaction—a violation of card network rules.

- A credit and debit card processor had its computer systems breached at a time when it was keeping on its computer system customer transactional data that should not have been stored after the transaction—also in violation of card network rules.

- Information brokers either sold data to unauthorized users or experienced breaches of their computer systems allowing unauthorized access to data.

- While in transit to storage or to a credit bureau, the data tapes of financial services companies have been lost by third-party couriers and airline baggage handlers.

- Seven employees of financial services companies and one government employee committed fraud by illegally selling bank account and credit bureau data to the owner of a collection company.

- A government agency recently alerted employees that they should remain vigilant for a period of time because they could become ID theft victims due to a breach at the agency. Other government agencies have also experienced breaches of their computer systems containing personal information on citizens.

- A media and entertainment company recently experienced the loss by a data storage company of computer backup tapes that contained employee data.

- At a number of major U.S. universities, computer servers containing student and faculty personal information have also been breached.

Only one of these breaches directly involved em-

A man in a dark suit and tie is shown from the chest up, looking down at a laptop. The scene is lit with a strong blue light, creating a high-tech or digital atmosphere. The man's hand is on the laptop's trackpad. The laptop keyboard is visible at the bottom of the frame.

BREACH

**Retooling Your
Customer Response
Program**

employees of a financial institution. But in every instance there is a financial institution customer at the end of the line. And if the data ended up being used to gain unauthorized access to an account or to perpetrate identity theft, your institution is on the front line in resolving the issue for your customer.

Because we cannot all be Harrison Ford and fight back as only he can, we as bankers must combine for a brute-force attack against breaches, both to prevent such breaches in our institutions and to recover from them after they have occurred.

That is where the compliance function comes in.

The Important Role of Compliance

In many financial institutions, and particularly in community banks, compliance has the personnel with the skill set to develop the policies and procedures around the customer response program that the Federal Financial Institutions Examination Council (FFIEC) agencies—minus the National Credit Union Administration (NCUA)—now require.

If compliance did not have a

role in putting together your institution's policy, at a minimum it would be prudent to ensure that your institution's program is complete.

The guidelines were issued in March 2005 and were effective upon adoption.

While the agencies recognized that some institutions would need additional time and took into account the good-faith efforts to develop a response program last year, we would anticipate that examiners will have higher expectations in 2006, and that institutions should for the most part now have their programs in place.

The guidelines require financial institutions to assess the risk of

- threats that could compromise customer information or customer information systems
- the likelihood and potential damage of such threats
- the sufficiency of systems and policies to control risk

Under the guidelines, after these risks are assessed, financial institutions must design programs to address them. At a minimum, financial institutions must consider access controls on customer information systems, background checks for employees with responsibilities requiring access to customer information systems, and response programs in the event of unauthorized access to customer information. Finally, contracts with service providers must require service providers to implement appropriate measures to protect against “unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.”

Financial institutions must also implement “risk-based” response programs to address instances of unauthorized access to customer information systems. Each institution's individual program will depend on the size and complexity of the institution and the nature and scope of its activities.

At a minimum, the response program should articulate plans to

- assess the nature and scope of the incident and identify what customer information systems and types of customer information have been accessed or misused
- notify the institution's primary federal regulator as soon as possible about any threats to sensitive customer information
- consistent with suspicious activity report (SAR) regulations, notify appropriate law enforcement authorities and

file SARs in situations involving federal criminal violations requiring immediate attention

- take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, including, for example, monitoring, freezing, or closing accounts while preserving records and other evidence
- notify customers when warranted

Notifying Customers of Breaches

A critical component of the guidance is the customer notification provision. When a financial institution becomes aware of a breach of sensitive customer information, it should conduct a reasonable investigation to determine whether the information has been or will be misused. If it determines that misuse of the information “has occurred or is reasonably possible,” it should notify affected customers as soon as possible. Customer notification may be delayed if law enforcement determines that doing so will interfere with an investigation and provides a written request for a delay.

The bottom line is that while bankers “get” information security and the vital importance of safeguarding customer information, many portions of the business and even government communities with which we do business have been involved in the recent data breaches affecting our customers.

And if the data ended up being used to gain unauthorized access to an account or to perpetrate identity theft, your institution is on the front line in resolving the issue for your customer.

Sensitive customer information means the customer's name, address, or telephone number in conjunction with the customer's

- Social Security number
- driver's license number
- account number
- credit or debit card number
- personal identification number or password to access the account

The definition of sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password.

The financial institution must notify only customers who were affected by the breach. If it cannot identify which customers were affected, it should notify all customers in the group if it determines that misuse of the information is reasonably possible.

The notice should be clear and conspicuous and delivered in any manner "designed to ensure that a customer can reasonably be expected to receive it." It should describe the incident in general terms and the type of customer information affected. It should also generally describe the institution's actions to protect the information from further unauthorized access and include a telephone number. The notice should remind customers to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution. The notice should also include, where appropriate

- recommendation to review account statements immediately and report any suspicious activity
- description of fraud alerts and how to place them
- recommendation that the customer periodically obtain credit reports and have fraudulent information removed
- explanation of how to receive a free credit report
- information about the FTC's guidance

The institution should also notify the nationwide consumer reporting agencies before sending notices to a large number of customers.

The States Step In

Not to be outdone, 21 states enacted security breach legislation in 2005, and as of this writing an additional six states have introduced or pre-filed bills for the 2006 session. While some states provide for an exemption for financial institutions that must adhere to the FFIEC guidelines, others do not. Closely evaluating any state laws that are relevant to your institution is thus important.

California has been the leader in imposing state security

breach provisions on financial institutions, and many of its provisions have been picked up by other states.

The FFIEC guidance specifically notes that the definition of the term "sensitive customer information" is broader than the scope of California's law. For example, California Senate Bill 1386 set a breach notification standard that pertained exclusively to unencrypted "computerized data." As previously noted, the guidance issued by the federal regulators expands the scope of sensitive customer information to include information in all forms.

Subtle but important language differences relating to the security breach notification trigger exist between the guidance and California law.

California law requires that an institution disclose any breach of the security of the system following discovery or notification of the breach, allowing little room for organizations to determine whether a security breach might actually result in harm to customers. On the other hand, the guidance applies a slightly broader, risk-based threshold. The standard for notification is based upon an organization's belief that a security breach of sensitive customer information "could result in substantial harm or inconvenience to any customer." This risk-sensitive approach to the actual threat of harm allows greater latitude for sound business decisions.

The required timing for notification also differs. The guidance defines notification timing as "as soon as possible." Conversely, California law sets a standard for timing as "immediately following discovery." Both the guidance and California law allow delayed notification when law enforcement is pursuing a criminal investigation, yet the standards regarding when and how an organization may be "cleared for notification" by law enforcement vary between the guidance and California law.

California also set a precedent for the manner in which organizations must notify those individuals potentially affected by a security breach. The California requirements are quite proscriptive, while the guidance provides a broader standard that suggests "clear and conspicuous" notification but does not prescribe the media or format.

For institutions serving California differences such as these have tended to create an environment where an institution is often forced to take a conservative approach when considering how and when to provide security breach notification, finding the "highest bar" across the states, so

Not to be outdone, 21 states enacted security breach legislation in 2005, and as of this writing an additional six states have introduced or pre-filed bills for the 2006 session.

Institutions should also be mindful of the regulatory requirements regarding incident response teams.

The FFIEC Information Security Workprogram Tier II examination guidelines require that examiners evaluate a financial organization to determine whether an incident response team

- contains appropriate membership
- is available at all times
- has appropriate training to investigate and report findings
- has access to backup data and systems, an inventory of all approved hardware and software, and monitored access to systems (as appropriate)
- has appropriate authority and timely access to decision makers for actions that require higher approvals

The FDIC also has specific examination guidelines regarding such teams, instructing examiners to evaluate the effectiveness of incident response practices by considering the following:

- establishment of appropriate escalation procedures to address varying alerts or incidents
- establishment of an incident response team to address incidents
- procedures governing actions to be taken based on incident reports received from outsource providers (e.g., Internet service providers application processors)
- Procedures for reporting suspected crimes and computer intrusions on suspicious activity reports (SARs)

to speak, for its overall customer response program. As additional states implement such laws, compliance becomes even more problematic.

Elements of a Customer Response Program

A customer response program is one component of an institution's overall information security program. Four key elements of any program include the development of your response team, the customer notification and assistance process, third-party service provider implications, and working with law enforcement.

Development of a Response Team

Your institution's incident response team allows you to have procedures and people in place when a possible customer information breach occurs. An effective incident response team is an institution-wide group that includes all affected lines of business. For example, if a customer's data has been compromised at a card processor, his or her checking account and debit and credit cards may be compromised. Rather than assuming a "siloed," single-business viewpoint, the institution can improve its response process by notifying all affected lines of business and units that can assist in responding to the event. When the entire scope of the compromise has been assessed, clear "ownership" can be established for leading your response efforts.

An incident response team shares many characteristics with your institution's other recovery teams. The incident response group may be closely aligned with the business continuity or disaster recovery teams. Just like other recoveries, the team can vary depending upon the incident's circumstances. Representatives

from legal, communications, information security, and the relevant business units are logical "first responders" to an incident.

As with other response planning efforts, a listing that contains multiple ways to contact team members is a helpful document. Institutions should also consider including contact information for security vendors, Web hosting companies, and other relevant technology providers.

Institutions may also want to review the resources available from the CERT® Coordination Center (CERT/CC), which has developed a number of tools to help companies develop computer security incident response teams.

Customer Notification and Assistance

An institution's customer notification program can be designed to ensure that all employees understand their role in a potential breach of security regarding sensitive customer information. Knowing what (and what not) to disclose in a breach scenario is vitally important to mitigate a host of legal, regulatory, and reputational risks.

The tasks involved in the customer notification process should be carefully defined and periodically tested. Another consideration for institutions is to have available customizable drafts of customer notification scripts, letters, and similar media appropriate for use across the organization's various delivery channels.

Notification Requirements for Third-Party Service Providers

Under existing information security guidelines, financial organizations are responsible for ensuring that third-party service providers take appropriate

**In general, the rule here is,
if in doubt, no matter
how minor the breach,
report it to
your regulator.**

measures to meet the objectives of the guidelines and comply with Section 501(b) of the Gramm-Leach-Bliley Act. According to the FFIEC, those measures must be included or referenced in the contract between the institution and the third-party service provider. Contractual language can also be inserted binding third-party service providers to similar security breach notification standards as required by the regulators and the relevant states.

Per the guidelines, the financial institution is responsible for notifying customers but may authorize or contract with its third-party service provider to notify the institution's customers on its behalf. The contract or a service level agreement can specify which party is responsible for notifying customers in the event of a breach.

Your institution may also consider—via a service level agreement or similar vehicle—a requirement that a third-party service provider promptly notify the institution of a breach using a special “hotline” or similar communication method. Other contract or service level considerations include specifying who is responsible for the customer notification process.

Institutions should also be cognizant of the dependencies of the third-party service provider on other third parties. As third-party service providers might rely on the services of a “dependent provider” to fulfill some aspect of contracted service to your institution, so too should the dependent provider be required to promptly notify the third-party service provider of any breach of proprietary information.

Notifying Your Regulator

Under the guidelines, a financial institution is required to notify the institution's primary federal regulator as soon as possible about any threats to sensitive customer information. This notification is required regardless of whether the institution ultimately determines to notify customers of the security breach. Most of the FFIEC agencies have delegated this process to the regional level, and while each region may handle the process slightly differently, an initial phone conversation will usually suffice as notification.

In larger institutions, considering the low threshold for notifying the institution's primary federal regulator, a process of reporting minor breaches (such as an account statement going to the wrong individual) in some sort of aggregated fashion may be able to be worked out with the agency.

In general, the rule here is, if in doubt, no matter how minor the breach, report it to your regulator.

Working with Law Enforcement

Among the components of the guidelines regarding response programs, the agencies state that an institution's procedures should include, consistent with the agencies'

suspicious activity report regulations, “notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing.” This provision is intended to be consistent with the existing SAR form instructions about when and how to immediately notify law enforcement, such as by telephone.

If law enforcement becomes involved in an institution's breach of customer information, they may request delays in notifying customers to conduct the investigation. It's advisable to involve legal counsel in any decision to contact investigative agencies when a security breach has occurred.

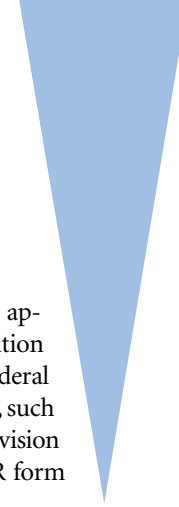
Tying It All Together

A successful customer response program can go a long way toward defending your institution and its customers from the potentially significant negative effects of a security breach.

After all, breaches happen. Just like Harrison Ford, we are vulnerable because we are human and we must deal with others who are human too, including some who would do us harm. The more swiftly you respond to a breach, the faster you can determine whether your customers are at risk. The better prepared you are to alert your customers, should they be at risk, the faster they can protect themselves. **BC**

ABOUT THE AUTHOR

Doug Johnson serves as the American Bankers Association's Senior Policy Analyst for Government Relations, where he is involved in a variety of public policy and compliance issues. He assisted in the ABA's recent release of a series of tools to deter bank robberies, assess information technology risk, deter phishing, and safeguard customer information in financial institutions. He represents the ABA on the Financial Services Sector Coordinating Council, which advises the federal bank regulatory agencies on homeland security and critical infrastructure protection issues. He is also an advisory board member of the Financial Services Information Sharing and Analysis Center, a private corporation that works with government to provide the financial sector with cyber and physical threat and vulnerability information, as part of the nation's homeland security initiative. Reach him by telephone at (202) 663-5059 or via e-mail at djohnson@aba.com.



Four key elements of any program include the development of your response team, the customer notification and assistance process, third-party service provider implications, and working with law enforcement.