Mitigating Cyber Threats To Banking Industry

Cyber-related crimes present high risk to banking industry. What types of cyber-crimes are risks specific to the banking industry and what can be done to mitigate them? This article addresses the most common cyber-crimes and provides some countermeasures for banks and financial institutions.

The E-Crime Watch Survey, conducted by *CSO Chief Security Officer* (CSO) magazine in co-operation with the U.S. Secret Service and the U. S. Computer Emergency Readiness Team (CERT) in 2004, estimated that "cyber attacks cost businesses more than $666 million in 2003. This estimate excludes ancillary losses due to identity and property theft. All told, this figure is believed to exceed $47 billion dollars". With plenty of companies using the Internet as marketing and sales tools, relying on high-speed communication networks, and encouraging real-time remote and a wireless mobile computing, the likelihood of loss and intrusion grows daily.

With the advent of computers (and especially the Internet) businesses are subject to threats of malicious activities and cyber-crimes. Cyber criminals use computers and technology to carry out the destructive activities that have been around for decades. Whether it is insiders or unknown intruders involved in hacking (i.e., the unauthorised use or attempt to circumvent the security mechanisms of an information system or network), cracking (i.e., breaking into a computer system), phishing (i.e., attempting to acquire identifiers and passwords), or phreaking (i.e., cracking a phone or communication network), as long as people are the weakest link, there really is no safe harbour from cyber-crime.

The banking sector consists of public sector, private sector and foreign banks apart from smaller regional and co-operative banks. In the market, various IT-based banking products, services and solutions are available. The most common of them are: Phone Banking; ATM facility; Credit, Debit and Smart Cards; Internet Banking & Mobile Banking; SWIFT Network & INFINET Network; Connectivity of bank branches to facilitate anywhere banking. The banking sector in India is on the verge of revolutionary changes in the way it functions and delivers its services to customers. The traditional "brick-and-mortar" bank branches are getting "networked" and becoming an integral part of an enterprise-wide banking platform, called "core banking solutions".

Cyber-related crimes, therefore, present an especially high risk to certain industries and types of businesses, including banking industry. Some examples illustrate the scope of the problem in the banking industry. A Phoenix-based bank accidentally allowed an employee of a small business to bilk her owner out of $91,000 in line-of-credit advances and $75,000 in credit card charges and cash advances. The employee used phishing and identity (ID) theft tactics to "spoof" the owner's identity to the bank and gained illegal access to credit and accounts. The owner lamented, "The bank could have nipped that in the bud right there, if they could have made one phone call to me." This example shows not only the new tactics employed by cyber criminals but also that banks suffer financial and reputation harm due to cyber fraud.

The Federal Trade Commission (FTC) reports that credit-related complaints have consistently ranked among the top 10 complaints made

– Dr. Madan Bhasin

(The author is Head, Accounting Department, Mazoon College, Muscat, Sultanate of Oman. He can be reached at madan.bhasin@rediffmail.com)

to the organisation for years. Research figures indicate that the total cost of fraud was as high as US$ 1.5 billion in 1999 and is growing at a phenomenal rate to an estimated US$ 39 billion for banks by 2005. It is now estimated that credit card fraud affects one in every 20-credit cardholders and costs consumers almost US$ 4 billion annually.

Some types of businesses, no doubt, are more susceptible to cyber-crimes. Vulnerable businesses include insurance, communications/media, defence contractors, health care, technology, high-profile businesses and financial institutions. In addition, governments are vulnerable too. The risks are probably as high or higher for the banking industry as for any other.

What kind of Cyber-Crimes are Commonly Perpetrated Against Banks?

The terms computer crime, high-tech crime, digital crime, e-crime and cyber-crime can be used interchangeably with electronic crime. E-crimes are essentially crimes where the computer is used either as a tool to commit the crime, as a storage device, or as a target of the crime. As a storage device, computers can either store information that will assist in the execution of the crime or information that is illegal for the owners to possess, such as stolen intellectual property. Computers are classified as a target if the information that they contain is altered or retrieved in an unlawful way, such crimes can range from amateur hacking to terrorism.

Perpetrators against banks can use several kinds of cyber-crimes. The most common are outlined in Exhibit-1. **Phishing** (pronounced "fishing") is growing rapidly. The Anti-Phishing Work Group (APWG) and the Federal Deposit Insurance Corporation (FDIC), both report that the financial services industry is the most commonly victimised industry. In fact, APWG says banks are about four times more likely to be victimised than the second highest victimised industry.

Phishing relies on the ability of the perpetrator to fool (or con) a victim, and that usually involves 'spoofing'. Spoofing is the imitation (or mimicking) of a legitimate Web site, e-mail or entity communication in order to trick the recipient into believing the communication or website is trustworthy. Thus, phishing involves the use of seemingly legitimate communications (that is, spoofed) to deceive bank customers into disclosing sensitive information, such as bank account information, social security numbers, credit card data, passwords or financial personal identification numbers (PIN). Most often, the purpose of phishing is to gain sufficient information to perpetrate a fraud.

Exhibit-1

Common Cyber Crime Risks for Financial Institutions

- Phishing
- Identity Theft
- Worms and Trojan horses
- Spyware
- Search engines/Google
- Blackmail
- Denial-of-service/distributed-denial-of-service attacks

For example, a perpetrator will create a fraudulent e-mail message that looks legitimate and arrives from an apparently trustworthy source. The legitimacy comes from copying the bank's logo or graphics from its Web site and inserting it into the document, along with official-looking signature files and contact information. The trusted source is not only the spoofed e-mail but a spoofed Web site as well. The e-mail, accompanied by a high sense of urgency, usually directs or links the recipient to a purported website of the spoofed bank. In reality, the person is being directed to an illegitimate website

where perpetrators will ask for information to serve their criminal intents. Often the spoofed uniform resource locator (URL or web address) will be similar to the real entity's address. According to the APWG, "the average time a spoofed site was online in 2004 was 6.2 days, and the longest was only 31 days." This trickery is facilitated by the fact that there is vulnerability in Microsoft's Internet Explorer that fraudsters can use to make it appear that the victim is at one Web site (URL) when in reality he or she has accessed a different and bogus one. One possible countermeasure is to use an alternate Internet browser.

A study shows that 76 per cent of all known phishing attempts occurred within the last six months. Another study (APWG) found that approximately three per cent of all adult Internet users revealed personal information to fraudsters.

ID theft is another major problem. The Federal Bureau of Investigation (FBI) has established a separate group, the Internet Crime Complaint Center (IC), to handle these types of crimes.

ID theft is another major problem. The Federal Bureau of Investigation (FBI) has established a separate group, the Internet Crime Complaint Center (IC), to handle these types of crimes. According to a study by Unisys, there is somewhat of a profile for ID theft victims. Consumers who have experienced ID theft tend to be under age 34 (30 per cent), with higher incomes (27 per cent, $75,000 +), college education (28 per cent) and reside in metropolitan areas (21 per cent).

One good definition of ID theft for financial institutions is provided by Visa: "ID theft involves manipulating or improperly accessing another person's identifying information, such as social security number, mother's maiden name, or PIN (rather than account number) in order to fraudulently establish credit or take over a deposit, credit or other financial account for benefit."

ID theft is closely associated with phishing. That is, ID theft is often made possible because of a successful phishing scheme, where sufficient information was captured to steal that person's identity and then perpetrate a fraud using that person's identity. ID theft, however, has been perpetrated successfully in the past without the use of phishing and still is perpetrated using other methods or means. ID theft is almost always employed as a means to commit other crimes.

Banks have generally had sound controls to secure this kind of sensitive and risky data. But that information can be gathered by physical means, such as Dumpster diving or social engineering, as well as cyber means, such as phishing, although phishing is clearly becoming more popular. Softer targets, such as bank branches, carry a higher risk of being the target for social engineering or ID theft.

Worms and Trojan horses are a significant threat to banks in terms of resources lost. A worm is a program (or algorithm) that replicates itself over a computer network and usually performs a malicious action, such as using up the computer's resources and possibly shutting the system down. It is similar to a virus. Unlike worms and viruses, Trojan horses do not replicate themselves but they can be just as destructive. One of the most insidious types of Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer. Another typical malicious use of a Trojan horse is to have it "sit" on a system and capture keyboard strokes and send them back to the perpetrator. This process provides the perpetrator the potential ability to steal passwords and IDs, especially for online banking.

A good example of worms and Trojan horses that target financial institutions would be the Bugbear family. **Bugbear** is a mass-mailing worm that spreads through networks. It also infects a select list of executable files. Bugbear possesses keystroke logging and backdoor capabilities and may even disable the system's anti-virus software. It specifically handles infections at financial institutions differently than other infections. This functionality will cause the worm to send sensitive banking data (files peculiar to banking computer systems and deliberately sought by the worm Bugbear) to one of 10 hard-coded, public Internet e-mail addresses. The sent information includes cached passwords and key-logging data. Other Trojan horses and key-loggers can be used in the same manner to retrieve user names and passwords for online financial accounts.

An emerging tactic for cyber criminals and crackers/hackers is **spyware**. A spyware is any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware ranges from harmless pop-up ads to the ability to record anything that happens on a computer and then transmit that data to a remote site. For example, WinWhatWhere software can record all keystrokes on a personal computer and send them to some remote location on the Internet.

Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet. Once installed, the spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers. During a recent consulting engagement, one of us removed more than 1,800 spyware objects on a single laptop computer.

Aside from the questions of ethics and privacy, spyware steals from the user by using the computer's memory resources and also by eating bandwidth as it sends information back to the spyware's home base via the user's Internet connection. Because spyware is using memory and system resources, the applications running in the background can lead to system crashes or general system instability. They have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications (such as chat programs or word processors), install other spyware programs, read cookies and change the default homepage on the Web browser—consistently relaying this information back to the spyware author who could use it for advertising/marketing purposes, sell the information to another party or use it to perpetrate ID theft. Spyware may sound like viruses or a Trojan horse. It is hard to tell the difference and there is not as strong an anti-spyware awareness, or as many anti-spyware tools, as is the case with antivirus software.

One key cyber-tool used by criminals is the **Internet search engine**, such as Google. For instance, credit card numbers are easily pulled. Bank account numbers can be found if placed improperly on the Web. In addition to sensitive information, sensitive resources can be obtained, such as secure login pages not published to the general public. This misuse of Google is referred to as "Google hacking".

DoS is intended to harm victims by bringing computer systems to a screeching halt, specifically servers, such as online banking servers that provide Internet access to bank transactions and data.

The list of risks also includes blackmail by perpetrators using technologies, as illustrated by CD Universe. A cyber-enabled criminal broke into its Web server and sold 300,000 credit card numbers and then blackmailed eUniverse (parent of CD Universe) to not publish them on the Internet, asking for a ransom of US$

100,000. When eUniverse decided not to pay the ransom, the cybercriminal, an 18-year old Russian cracker, published 25,000 credit card numbers the next day on the Internet, making good on his threat. eUniverse Chairman Brad Greenspan replied to that act in a statement: "Refusing to bow to this new breed of cyber-criminals, we have taken a stand against a new form of online blackmail on behalf of all legitimate e-commerce retailers." True, but it severely crippled the level of business for CD Universe for some time, threatening its very existence.

Generally, a bank's goal is to adopt a customised set of procedures and practices that enable control to be exercised over critical information and technology assets in a cost-effective manner.

Finally, there is the risk of **Denial of Service** (DoS) attack against online banking. DoS is intended to harm victims by bringing computer systems to a screeching halt, specifically servers, such as online banking servers that provide Internet access to bank transactions and data. When financial institutions' online banking services are down, not only are business operations disrupted but also the cyber-enabled perpetrator might gain publicity from his or her act—a common goal of such attacks. Distributed denial of service (DDoS) is a modified DoS where multiple attacks are launched simultaneously from various innocent client computers to a single target, flooding the computer server system and locking it up. DoS/DdoS attacks have less of an impact on financial institutions and are less devastating to the overall entity than the other forms of attack.

What Banks Can do to Protect Against Cyber-Crimes

With the growing cyber-crime threat and increasing institutional liability, there is no other option for banks but to be 'proactive', logic made all the more certain given that more than 30 percent of successful hacks are committed by employees or related persons. However, contrary to conventional thinking, any bank taking the lead in enacting a fist-line of defence needs to start with "Senior Management," not the Information Technology (IT) Department. The concern, commitment, and control of management are critical to adopting, funding, and enforcing an effective protection scheme that may be fully implemented in the workplace.

That is not to say that internal IT or contract technology personnel have no role to play, but simply directing IT personnel to install a firewall or regularly change passwords would not be a cure-all. Like any other form of corporate security—from sign-in sheets to identification badges to biometrics—it only takes one motivated person dedicated to breaching a system's weakest point to overcome a seemingly impenetrable chain of protection. A bank simply cannot afford to make the mistake of deploying anything less than a comprehensive top-down strategy to enable a reliable system of computer network security.

A Protection Strategy

Generally, a bank's goal is to adopt a customised set of procedures and practices that enable control to be exercised over critical information and technology assets in a cost-effective manner. A Software Institute categorised a comprehensive approach to physical, technical, and administrative security controls as follows: *preventive* (i.e., secure card readers, encryption, spyware, and company policies and procedures); *detective* (i.e., archival seals, log messaging controls, and regular e-audits); *deterrent* (i.e., closed circuit cameras, rejection after incorrect password use, and multi-departmental approvals); *corrective* (i.e., isolation of servers, updated firewalls and procedures, segmentation of space by function); and *recovery* (i.e., dual

data sets, integrity services for repairs, and law enforcement and legal action).

Apart from these formal constructs, banks also need to be **practical**. Adopting procedures to deal with suspicious employees, taking actions to address a lack of internal forensic computer expertise, purchasing sufficient liability insurance coverage for adverse electronic events, and implementing crisis teams are all basic issues that banks need to consider in addressing any comprehensive security system. Technical consultants can help provide any bank with a complete blueprint for action on this front.

However, banking industry can use some **basic protection methods** and specific defensive tools to minimize their risks from cyber-crimes. In general, a bank needs to use some sound logic and not to overreact or panic in developing protection mechanisms. Two good places to start are an effective risk assessment and a review of the policies and procedures related to security.

The **risk assessment**, if done appropriately, will direct the rest of your actions and lead to effectiveness. Get some professional assistance, if necessary, but make sure your bank has analysed all possible threats and risks associated with cyber-crimes and similar malicious activities. Even when your resources are limited, identifying all the risks is inherently valuable. That allows management to 'prioritise' the risks with high probability and high impact or costs (if a crime occurs). This prioritised list then provides a cost-effective means of mitigating the risks.

Second, the bank can implement prevention techniques, tools and policies. The tools would include technologies to protect the bank's system and network from malicious objects and attacks, such as firewalls, intrusion detection system, anti-virus software and anti-spyware procedures. It also would include a strong public education campaign to minimize the risk of phishing and ID theft.

Third, a bank should ensure it has a sound business recovery plan in its policies and procedures in case an attack occurs and succeeds. Several things can cause a bank to lose its computers and information systems, including system failures, disaster (man-made or natural), hackers/crackers and other cyber criminals. An effective business recovery plan will allow a business to recover from any of these unfortunate events. It is essential that the recovery system, especially data recovery, be tested before relying upon it.

Fourth, develop an incident response plan as part of the policies and procedures, if applicable. An incident response plan should be developed for any risk that exceeds 'minimum' risk. What if some cracker or cyber-criminal attacked your bank successfully and did the one thing that has the highest public risk for the bank (for example, stole thousands of credit card numbers and PINs, wiped out your hard drives, stole the corporate identity, etc.)? How would your bank respond to that attack and the resulting bad publicity? There is no substitute for the preparation and planning for such an event, and an appropriate incident response plan does just that.

The more cases of cyber-crimes over the ICTs, especially through the fastest growing medium like the Internet, the more voices for regulating them in whatever forms.

Fifth, education (viz., training, seminars, etc.) is critical to developing an effective level of awareness regarding the types of risks, knowledge of the "red flags" for which to watch, and a vigilant defense necessary for at-risk businesses, such as banks. Education includes both consumers and employees, and their ability to recognise the types of cyber-crimes and respond appropriately to each. A

key control point in detecting and preventing cyber criminal tactics (for example, phishing, ID theft) is the bank's own employees, especially frontline staff (for example, the information systems help desk).

Last but not least, banks can use some specific information technology (IT) or information systems (IS) countermeasures to mitigate the risk of cyber-crime. For example, a U.S. banker recommends "fraud detection software, voice print recognition, and smart chips to replace magnetic stripes on cards." Similarly, the FDIC recommends "scanning tools, e-mail authentication (an example would be digital signatures) and user authentication (an example would be voice print)." The FDIC report "Putting an End to Account-Hijacking Theft" provides extensive details on these suggested IT defences. In the same report, the FDIC recommends additional steps to reduce online fraud:

- Upgrade existing password single-factor authentication systems to two-factor systems.
- Use scanning software to proactively identify and defend against phishing. Employ fraud detection software to identify account hijacking.
- Strengthen educational programs to help consumers avoid online scams.
- Plan a continuing emphasis on information sharing among financial institutions, government and IT providers.

The more cases of cyber-crimes over the ICTs, especially through the fastest growing medium like the Internet, the more voices for regulating them in whatever forms. Some countries, thus, began to accommodate such voices (or demands) through revising the existing laws and/or issuing new legislation—or 'cyber-laws'. The scope of cyber-laws is yet unclear in many countries although it can be interpreted at large in two ways: One is for the relevant legislation dealing with or regulating converged computer, telecommunications and multimedia or broadcasting in such cases as the Multimedia and Communications Act, Malaysia; the other is for those tackling the emerging cyber-crimes in such cases as the Information Technology Act in India and the Convention of Cyber-crimes just adopted by the Council of Europe. Despite these laws and great intentions, significant legal limitations exist.

Conclusion

A bank, therefore, needs a broad strategy of prevention. Please remember: "No one method can protect a bank against all types of cyber-crimes and cyber-enabled perpetrators." Because of the high-level of risk in banking related to cyber-criminal activities, banks must maintain constant vigilance and diligence to be aware of the risks, assess and prioritise the risks, and take appropriate actions to mitigate the risks. One of the general issues in the development of cyber-laws is the nature of cyber-space itself, which is new and young. Traditional laws, thus, will not be effective in tackling the various types of activities conducted on the cyber-space. For example, deception of computer, or theft of electronic data cannot be dealt with under the traditional penal laws in many countries. That is why certain countries like India, Malaysia and others began to enact the new "Information Technology Act" and "Digital Signatures Act," respectively. The other issue is jurisdiction of the courts and applications of the laws due to the nature of the cyber-space beyond national jurisdiction. In order to survive and grow in a global competitive scenario, time has already come when the security aspects of the banks must be dealt with on a priority basis. ❐

The other issue is jurisdiction of the courts and applications of the laws due to the nature of the cyber-space beyond national jurisdiction.