BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **6**, No 2

Sofia • 2006

Effectiveness of the Information Security in the Banks

Rosen Kirilov

UNWE, 1113 Sofia
E-mail: rosenkirilov@mail.bg

Abstract: *Digital technology provides us with exciting new tools that can have a major impact on education, health, commerce, and other sectors of civil society. This technology benefits all countries and people, but has a special attraction for developing countries in that it can help to accelerate their integration into the world economic community. This paper present information security in the banks and the effectiveness of the computer information systems and security policy.*

Keywords: *effectiveness, information technologies in banks, security.*

I. Introduction

In small organizations, provisions for IT security may also be quite simple, with each person holding responsibility for his or her own computer and files. However, for somewhat larger groups, groups that are engaged in commercial transactions, or groups that maintain confidential data for customers or public citizens, the need to establish formal security policies and procedures becomes more important. When managers and their staff consider the issue of IT security, whether they are operating businesses, non-profit organizations, or government agencies, they will all have similar concerns. Each group will want a certain level of security for their data, procedures that are clear and easy for employees to follow, the ability to retain and build on knowledge of customer needs, and an understanding of how their security policy is faring in a given operational environment. In addition to these general needs, each type of organization has special concerns related to its mission and goals. Managers must emphasize information security policies in the appropriate context in order to pursue stated objectives effectively. It is also important to understand the costs involved with implementing good security practices. Security procedures and technologies are an investment and should be evaluated against the costs of potential losses.

Our survey in the Bulgarian banks reveals that 75% of organizations say information security is of high importance for achieving their overall objectives. 73%

of banks identify risk reduction as their top influencer for information security spending. Even so, nearly 60% of banks say they rarely or never calculate return on investment for information security spending. These statistics illustrate the fact that all, no matter how large and seemingly well-off, feel the pressures, both psychological and financial, that come from threats to IT security.

If you are running a small or medium sized business, your top priorities are profitability, business continuity, sustainability, and customer service. SMEs are also bound by local, regional, or national laws and may be accountable to a range of authorities, depending on the business that they are engaged in and the country's overall business environment. Security will be focused on protecting the enterprise and its customers from fraud and costly malicious attacks on their systems and services. In addition to computer crime and network security, data protection is also important to SMEs and encompasses two main areas: enterprise data protection from corporate spies or attackers and customer data protection, including credit card and transaction information.

In non-profit organizations, your managers and employees are focused on effectiveness in the field, coordination with communities and partners, and reputation. Systems may be widely disbursed and are often of lesser quality due to the budget constraints present in the non-profit world. In addition, the staff may be less experienced with technology and thus will be facing a substantial challenge as they seek to provide uninterrupted service to their constituencies and maintain a positive image to their donors, overseers, and peers.

As with non-profits, budget constraints, disbursed networks, and a wide range of technological skill are present in university systems. Universities may face a greater number of internal threats as students may find hacking the institutional system an engaging pastime. In addition, universities may be operating under a unique set of internal policies and also need to comply with government regulations. In the university environment, personal data protection is extremely important, as student files include much sensitive information including identification numbers, health records, and academic transcripts. Potential attackers could steal, modify, or destroy such data, causing serious damage to the credibility and effectiveness of the university system.

In government agencies, IT deployments may be assessed in terms of efficiency, ease-of-use, and ability to link up with other departments and agencies as needed. While profitability is generally not relevant in the governmental context, like non-profits, there are often budget controls that limit the agency's ability to acquire the latest in hardware and software security. At the same time, governments must be keenly focused on data protection in targeted environment, as their databases contain sensitive information on individuals, including personal identification, health, criminal, and tax records. Unfortunately, even in industrialized countries, data protection in government agencies lags behind and suffers from antiquated systems, inadequate funding, and overworked staff who lack core competencies in IT security. Like businesses and non-profits, the government must be concerned with its public image after hacking incidents or other security breaches are brought to light in the media.

In a report on IT in developing countries, the UNDP [1] outlined some of the promises and challenges facing individuals and organizations in the information age. The World Bank has been producing a series of reports on specific topics in information technology development and deployment [2]. Although the enterprise technology experiences in the industrialized world are different in some ways (scale, costs,

knowledge base of the personnel), there are some lessons to be drawn from their strengths and weaknesses in the area of IT security. Large enterprises are fewer, have specialized capabilities, and deeper pockets. However, there are still tensions between Chief Security Officers as managers of cost centers, Chief Financial Officers as cost controllers, and other branches of the organization (Chief Information Officers, Sales and Marketing, production). Without an overarching mandate to create a secure IT environment, each group could develop an approach to security that is driven by its own mission, goals, and operational targets. While these varied approaches might lead to some areas being over-secured and other being under-secured, clear communication from top-level management will emphasize that sound security practices are aligned with the well being of the organization. The technology policies and implementations required to operate a safe and secure system for the enterprise are a necessary part of meeting core business objectives effectively. Small and medium sized enterprises have fewer resources to deploy, a flatter management hierarchy, and heavier reliance on the knowledge base of all employees. In SMEs, the business processes may be more transparent than those in a larger organization and there are special security risks inherent in a structure where so much corporate information is out in the open, for all employees to see. In businesses that are not focused on technology, there may be vulnerabilities to an employee or consultant who is more technologically savvy than the company managers. In a technology-focused company, there is the danger that critical intellectual property may be insufficiently protected from theft or destruction.

As a safeguard against such problems, all SMEs should conduct a complete review of their mission, goals, competencies, and information systems. If they are working in areas that may create security risks for others, developing emerging technologies, for example, they should examine the likely threats to their customers' security and develop mitigation plans. If they are working in areas that will face government scrutiny, offering products and services in telecommunications, for example, then they should understand when and how they may be legally responsible for adhering to government mandates. An Internet Service Provider is an example of a business that runs both types of risk. By hooking customers up to the Internet, they are creating potential security risks for that customer's data and equipment and by providing digital content and a means of communication, the ISP is subject to state and federal regulation. If one adds the capacity for e-commerce, the potential gains and attendant liabilities are substantial.

In spite of the challenges, entrepreneurs and managers in the public and private sectors in developing countries are investing in new information and communication technologies, including e-mail, the Internet, wireless telephony, and business software to assist in running their day-to-day operations. The advantages in efficiency, outreach, and cost savings in these new devices and services are clear:

1) they improve business communications with customers, suppliers, and partners;

2) they enhance the ability to access large quantities of information quickly and cheaply;

3) they provide a means to expand data protection and management capabilities, resulting in better record keeping for financial managers, better customer analysis for sales and marketing managers, and better production statistics for line managers.

However, these improvements are not without risk, both the physical assets and to less tangible information assets. Information System Audit and Control Association has partnerships in 60 countries and provides cases from various countries, and programs, all available as open source. ISACA also offers an audit and control framework for organizations and includes checklists for outsourcing situations. Whether conducted and controlled in-house or through outside vendors, developing and maintaining strong security infrastructure, policies, and procedures is a balancing act for most enterprises. Executives, managers, and policy makers must weigh the risks and set a standard that balances the investment in security with the official objectives and bottom line growth of the company. Once a company has achieved the desired level of security, the management must not forget the importance of maintaining up-to-date systems and performing regular audits of the security plan. Changes in computer and networking equipment, from proprietary to Open Source software packages, for example, will require a complete review of the security blueprint. In short, security is an art form, rather than a science, and requires the coordination of many creative thinkers to ensure its successful impact on an organization and society as a whole.

II. Information security in the banks

This chapter, defines, policies, processes, and an overall infrastructure that can foster a secure electronic environment for the financial services sector. It is intended for policy makers working with financial services providers, especially executives, chief information, and security officers. The technical sections should be of special use to those who administer electronic security systems, bank examiners who evaluate the adequacy of electronic security, and those who deal with the associated day-to-day risks inherent in electronic transactions.

Many authors identified electronic security as crucial to enabling electronic finance to meet business and consumer expectations and deliver the benefits provided by technology and leapfrogging [3]. E-security touches the heart of the new economy; the potential benefits to global markets and the international community are substantial. However, the process of building a global electronic economy merits deep discussion of emerging business and policy issues: how should we define and protect privacy?, what do trust and confidence mean in a digital environment?, how can one determine the appropriate level of security and how can one measure the return on the security investment?

Due to the ever-changing nature of technology, this paper does not treat all these issues nor does it attempt to provide definitive answers. Rather, it offers a view of what has transpired to date, the gaps that are opening in the electronic security area, and some possible approaches for bridging those gaps. It also acknowledges some of the efforts underway around the world aimed at resolving these issues.

Broadly speaking, electronic security is any tool, technique, or process used to protect a system's information assets. Electronic security enhances the value of a network and is composed of soft and hard infrastructure. The soft infrastructure components are the policies, processes, protocols, and guidelines that protect the system and the data from compromise. The hard infrastructure consists of hardware and software needed to protect the system and data from threats to security from

inside or outside the organization. The degree of electronic security used for any activity should be proportional to the activity's underlying value. Appropriate security measures will mitigate (but not eliminate) the risk for the underlying transaction, in proportion to its value. *Electronic security will require more attention as new technology creates new risks and as technologies converge.*

E-finance is the use of electronic means to exchange information, transfer signs and representations of value, and execute transactions in a commercial environment. E-finance comprises four primary channels: electronic funds transfers, electronic data interchange, electronic benefits transfers, and electronic trade confirmations. Although e-finance offers developing market economies an expanded opportunity for commerce, the capability poses a number of serious risks. All four channels of e-finance are susceptible to fraud, theft, embezzlement, pilfering, and extortion. Most of the commerce-related crimes that take place over the Internet are not new fraud, theft, impersonation, and extortion demands have plagued the financial services industry for years. However, technological advance opens up new dimensions of depth, scope, and timing. Technology creates the possibility for crimes of great magnitude and complexity to be committed quickly and anonymously. In the past, stealing 50,000 credit card numbers would have taken months, perhaps years, for highly organized criminals. Today one criminal using software tools freely available on the Web can hack into a database and steal that number of identities in seconds. Recent surveys suggest that, 57% of all hack attacks were initiated in the financial sector last year. The results of well-publicized security breaches range from financial and reputation loss to a potential backlash against electronic transactions stemming from mass consumer distrust of the e-finance and e-commerce media. The network-mediated economy presents unparalleled opportunities for both the creation of wealth and the theft or destruction of it. In assessing its promises and weighing these against potential pitfalls, policy and decision makers should educate themselves about the role that e-security plays in ensuring safe and reliable business transactions via the Internet.

The electronic security industry is growing and globalizing; it will present public policy challenges in the areas of competition policy, potential conflicts of interest, and certification.

E-security companies and vendors generally fall into three categories: access, use, and assessment. Today's industry includes companies that provide active content monitoring and data filtering, develop intrusion detection services, place firewalls, conduct penetration tests to expose hardware or software vulnerabilities, offer encryption software or services, and create authentication software or services that use passwords, tokens, keys, and biometrics to verify the identity of the parties or the integrity of the data. In addition to e-security, many vendors supply a multitude of interlinking services to the e-finance providers in various countries. These services include hosting companies, Internet Service Providers (ISPs), and providers of financial services. Telecommunication companies in emerging markets are often the key providers of cellular, satellite, and microwave services as well. Such companies may also supply hosting services and de facto money transmission services. In some cases, they may also provide certain electronic security services. The cross-linking ownership of the e-security and e-finance industries raises complex questions of competition policy and potential conflicts of interest. In the case of competition policy, do the multiple roles played by telecom companies act to inhibit competition, particularly in emerging markets where the technical expertise to provide such services often resides

in these companies? What about assuring the integrity of the services provided and company policies on reporting security breaches promptly and accurately? Moreover, outsourcing trends in this industry highlight the importance of reviewing the extent of downstream liability involved with this complex set of vendors. Typically, contracts between financial entities and their providers use service-level percentages as a performance guarantee on a sliding-cost scale, but they do not build in sufficient remedies to address product performance from a security perspective. The public interest case for regulation of electronic security within the financial services industry must be recognized. Important trade-offs exist between electronic security and such areas as costs, quality of service, technological innovation, and privacy. Formulation of regulation and policy needs to take explicit account of these trade-offs. Traditionally, the telecommunications industry has been regulated as being essential to public health, interest, and welfare. Hence, a core component of its regulatory model was to expand service to give everyone access. In many countries, access to basic service is now considered a necessity of modern life. Historically, the financial services industry has been regulated by the premise that trust and confidence are paramount to the orderly movement of trade, goods, and money. And, given that a special trust is conferred on financial entities, they must conduct their business in a safe, sound, and prudent manner. Convergence of the telecommunications industry and the financial services sector through the Internet heightens the importance of and the necessity for sound public policy and informed regulation to ensure that government, business, and people continue to have access to secure financial services. Efforts to develop public policy to improve or establish electronic security measures should take into consideration the following six important pillars:

II.1. Robust supervision and prevention, to creates better incentives to implement appropriate layered risk-management systems, including electronic security for financial services providers

In addition to monitoring the payments system and supervising money transmitters, there would be a benefit to revisiting the regulatory, supervisory, and preventive approaches to ensuring security for financial services providers. This is particularly true for businesses that engage in electronic banking or provide other online financial services. The new Basel guidelines for capital, especially those dealing with operational risk, do not address the problem of measuring either the risk to reputation or the strategic risk associated with electronic security breaches. Hence, there is a question of how best to measure a bank's operational risks when the information about computer security incidents is not accurate and when defining reputation damage is difficult. Given the problems involved in measuring capital adequacy in cases of electronic security risk, one effective approach might be to use the examination process to identify and remedy electronic security breaches in coordination with better incentives for reporting such incidents. In addition, authorities could encourage or even require financial services providers to insure against some aspects of e-risks (e.g., denial of service, identity theft) that are not taken into account within the existing capital adequacy framework. As the private insurance industry becomes more active in this field, this approach may be feasible, subject to the overall soundness and health of the insurance industry and its structure in emerging markets. The legal or regulatory framework could create incentives for hosting companies, application service providers, and software, hardware, and e-security providers to be accountable to the

financial services industry. The Basel Committee on Banking Supervision's Electronic Banking Group (EBG) was formed to make recommendations for needed additions, changes, or improvements in supervision and examination to accommodate the new technologies. In 2001 the EBG released Risk Management Principles for E-Banking, which includes specific principles calling for proper authorization and authentication measures, and internal controls and comprehensive security of e-banking assets and information. The areas of supervision and examination will undergo major reorientations over the next few years. Just as the security industry experienced a paradigm shift with the mass introduction and dependence on PCs and the Internet, so must bank supervision realize that the center of gravity in the financial services industry is changing. One key issue facing most countries is the need to improve information exchange between regulatory and law enforcement agencies. Many countries have several agencies for gathering critical information, but often the data is not shared by these agencies or with the agencies of other nations (sometimes for legal reasons). The issue of information exchange between agencies in both domestic and international contexts is beyond the scope of this Paper. However, as governments try to leverage scarce resources in order to regulate and battle crime in the electronic environment, information sharing and international cooperation are key issues.

II.2. A framework within which private insurance companies can insure against and monitor e-risk, thereby helping to improve standards in this area via the underwriting covenants they require

Financial supervisory agencies are still developing regulatory standards. Due to the difficulties inherent in monitoring complex transactions taking place over rapidly changing technological infrastructures, it is important to seek complementary private solutions to monitor risks. The insurance industry already is playing a role in this area despite the defects present in the information that is used to price e-risk coverage. Over the next few years, in the United States market alone, the growth in e-commerce liability insurance and e-risk coverage may total as much as $2.5 billion annually. Still in its early development, insurance related to e-commerce liability and e-risk has problems in firstand third-party coverage. The pricing of cyber-risk insurance is also in need of further development, but to accomplish this, the insurance industry needs a better base of information on security breaches and associated risks. Current underwriting practices for this form of insurance have paid insufficient attention to the special risks that wireless technologies bring to the delivery of financial services. Insurance providers could require that explicit electronic security standards for wireless technology be identified and used to mitigate these risks before they underwrite e-risk policies. The global insurance industry can serve as an important force for change in electronic security requirements. First, it can strive to improve the minimum standards for electronic security in the financial services industry. The global insurance industry could advocate the use of enhanced layered electronic security as a business prerequisite, for example. Second, insurance companies could require that financial services entities use vendors that meet certified, industry-accepted standards to provide electronic security services as a way of mitigating their risks of underwriting coverage. Third, insurance companies could encourage regulators to require that financial services entities provide and improve the quality of data and information on incidents so they can conduct better actuarial analysis on e-risks and return on investment. Finally, the industry could promote solutions that require e-security vendors and other

e-enabling companies (hosting, etc.) to engage in risk sharing and to bear appropriate liability for security breaches.

II.3. Digital signatures

Both public and private entities should work cooperatively to develop standards and to harmonize certification schemes. Two categories that require particular attention in terms of certification deal with electronic security service providers and transaction elements. One possible approach in securing e-finance would be for financial regulators to require licensing of vendors that directly affect the payment system. Another approach would be to require the industry to certify vendors that provide electronic security services. Recently the security industry has developed a Security Expert certification. By using a certification approach, the industry benefits by providing consumers with a recognizable structure, accountability between the industry and its experts, and a means of separating the approved expert from the self proclaimed expert. It also elevates the field of security to a professional status and creates an incentive for the industry to raise and protect standards. A second area to consider is the certification of transaction elements such as electronic signatures. Certification can add value to a transaction, depending on who or what provides the certification and on the elements that are being certified. Certification may be offered by a governmental entity, such as a post office, or a private entity, such as a bank. Each of these scenarios presents unique structural and governance issues. In many countries private companies (financial services providers or non-financial companies) may be better equipped to provide the information infrastructure required to act as certification agents or to provide cross-certification. The essential element to a successful certification scheme is that certification structures located in different jurisdictions must provide the same attributes to the transaction consistently and that a certifier's scope of authority and liability must remain uniform across jurisdictional borders. Although the use of PKI technology and certification authorities is often touted as the only accepted means of ensuring security, it is necessary to consider the costs and the cumbersome structure associated with PKI, as well as the legal inconsistencies associated with certification authorities. The practical element is that the solution be applicable across borders in terms of scope and liability, no matter what technology is used to perform the function.

II.4. Information sharing

The lack of accurate information on e-security incidents is the result of the lack of knowledge or motivation to capture the data, measure it, and share it. Electronic security would improve worldwide through the enhancement of national and cross-border arrangements to facilitate sharing by financial services providers of accurate information on denial-of-service intrusions, thefts, attempted fraud, and so on. Failure to share information not only limits awareness but, even more important, it can limit the development of private sector solutions (including insurance). This lack of information may even serve to increase the cost to companies and financial services providers of insuring against such risks. Greater public-private sector cooperation is needed in this area. For example, BITS' Security and Risk Assessment Steering Committee is addressing security, safety, and soundness in existing and emerging payments, electronic commerce, and related technologies through the establishment of a Financial Services Security Lab. This Lab facilitates information exchange on security issues in the financial services industry. Furthermore, the Internet Security

Alliance, the Forum of Incident and Response Security Teams, and the Computer Emergency Response Teams set up in various countries have shown that cooperation results in greater information sharing among law enforcement and private providers of financial services. A common element in all these programs is a reliance on confidentiality and trust; as a condition of receiving accurate information, the law enforcement and academic entities do not divulge the identity of respondents. In this area, the role of multilateral agencies to facilitate cooperation deserves examination. It is axiomatic that the more "connected" the economy becomes, the more important it is for each element to bear its portion of the burden. Today's financial services industry was founded as an integrated system. The technological changes of the past decade have expanded and heightened the interdependencies of that system.

II.5. Education of citizens, employees, and management on security issues

Statistical analysis reveals that in many countries throughout the world, more than 50% of electronic security intrusions are carried out by insiders. An undereducated workforce is inherently more vulnerable to internal attack. By contrast, a well-educated workforce that is conscious of security issues can effectively add a layer of protection. Educational initiatives could be targeted at financial services providers (both systems administrators and management), at various agencies involved in law enforcement and supervision, and at users of online financial services. Initiatives might include the following:

- improvement of awareness and education of financial sector participants about cyber ethics and appropriate user behavior on networked systems;
- creation of institution-wide e-security policies on appropriate behavior and the corresponding channels for reporting intrusions or incidents in close coordination with any effort to improve worldwide information on intrusions;
- development of awareness in the banking community in emerging markets about the need for "incident response plans" in case an incident transpires;
- facilitation of cooperation and transfer of know-how among law enforcement entities, financial intelligence units, and supervisory agencies in developed and emerging markets via such devices as more active exchange programs between personnel;
- design of focused courses for examiners under the auspices of the Financial Stability Institute or other training centers;
- development of a cross-border university outreach program to promote the training of future e-security professionals, while also improving the education of users of online financial services.

II.6. A layered security structure

Twelve core layers of proper security are a fundamental component for maintaining the integrity of data and mitigating the risks associated with open architecture environments. The twelve-linked chain defines what security should be online. The network is only as secure as its weakest link.

Countries adopting electronic banking or electronic delivery of other financial services (e.g., distribution and trading of securities) must consider electronic security concerns as they develop their laws, policies and practices. They must promote the use of security to protect back-end and front-end electronic operations and should reform their criminal laws to address cyber crime.

In the policy design process, an e-finance legal framework should take the following areas into accounts:

- electronic transactions and electronic commerce;
- payment systems security;
- privacy;
- cybercrime;
- anti-money laundering;
- enforcement infrastructure;

Together, these six areas of policy, law and enforcement should address the *basic relationships* among all participants and the *transactional activity* that flows through the payments system. A cornerstone of an e-finance legal framework is to recognize the legal validity of consumer electronic signatures, transactions, or records. The legal framework should prefer technology neutral solutions, provide basic consumer protections for electronically based transactional activity, promote interoperability, and address evidentiary issues.

Electronic transactions law should define what is meant by an electronic signature, record, or transaction, recognizing the legal validity of each element. The policy should be especially careful in defining an electronic signature. Definitions should be technology-neutral to the greatest degree possible, in order to allow various technical solutions to enter the marketplace.

Development of policy for payment systems security should consider all entities that directly affect the system. All such entities should operate in a secure manner so as to protect the integrity and reliability of the system. Further, policy could require timely and accurate reporting on all electronic -related money losses or suspected losses and intrusions. And finally, policies could require that the financial institution and related providers have sufficient risk protection.

Privacy law should encompass data protection and use, consumer protection and business requirements, and notices about an entity's policy on information use.

The European Union continues to be the leader in providing privacy protection to its citizens with the 1995 EU Directive on Data Protection. At a minimum, the privacy law should embrace the fair information practice principles, including notice, choice, access, minimum information necessary to complete the transaction.

Every nation should have in place laws addressing abuses of a computer or network that result in loss or destruction to the computer or network, as well as associated losses. The law should also provide the tools and resources needed to investigate, prosecute, and punish perpetrators of cyber crimes. An example of such laws and directives may be seen in the Council of Europe's Convention on Cybercrime.

These statutes should define money laundering and encourage international cooperation in the investigation, prosecution, and punishment of such crimes, giving special attention to money laundering threats inherent in new or developing technologies.

Perhaps as important as the legal framework will be the need to enforce the provisions of e-security laws within and across national boundaries. Many different types of computer intrusions originate through activities conducted in countries with weak legal and enforcement regimes for electronic security, making international cooperation essential.

Payment systems are a critical component of any financial system. Policies to mitigate risk to payment systems should address the following five problems:

- the definition of money transmitters;
- reporting requirements;
- regulation;
- warranties, indemnification, and liabilities;
- security requirements for service providers.

A money transmitter is any commercial enterprise engaged in the transfer and exchange of monetary instruments and currency. Often these non-depository entities are involved in the “money service business” and serve as third-party automated clearinghouse providers. In considering the security of the electronic payment system, regulators should recognize that a new paradigm for money movement has evolved in a sophisticated IT environment. The significant amount of money that flows around banks instead of through them has a significant impact on the global payment system, monetary policy, and economic forecasting.

The failure to report security incidents, particularly in the financial services area, enables further engagement in unsafe and unsound activities and further losses to those who use such payment systems without check or prevention. One approach is to place an affirmative duty on executives to report incidents.

Regulators should consider how broadly to extend supervision and enforcement over transmission vehicles. The primary reason cited by most people for refusing to use electronic transmission vehicles is fear that the information is not adequately protected. Proper protection could strengthen consumer confidence and market discipline, paving the way for greater use of electronic financial systems.

Financial institutions could require warranties and indemnifications from businesses that create software and hardware or supply it to financial services providers. They also could require the companies that provide these products to be liable if losses occur as a result of software or hardware “holes.” Entities providing services or products to the financial services industry could, perhaps, be held to a higher standard of care or The Council of Europe, Convention on Cybercrime [3], required to explain up front that its product is not configured or otherwise appropriate for use in this sector. A variation on this solution is to require a disclaimer on hardware or software stating that it should not be used to create, move, or store confidential, privileged, or sensitive information and that if it is used for those purposes the manufacturer cannot be held liable.

Service providers to the financial services industry also could be held to a higher standard than those not interacting directly with that industry. Again, this effort would go a long way toward building trust and confidence.

III. Risk evaluation and loss analysis in the banks

This chapter covers security risk evaluation and loss analysis in a business context. We consider a range of security threats, their potential origin and action, and consider the severity of their effects on our day-to-day operations. We outline the cornerstones of a sound security policy and explain the basic principles of loss analysis, should a real security incident take place.

All businesses, whether they are large or small, are operating in an increasingly global environment. Advances in communications and transportation networks in the last century have brought customers and markets closer together and it is now possible,

at relatively minimal cost, to ship products to buyers in all corners of the world. In this international context, executive and managers must consider the range of threats to their enterprises. Since the late 1990s, there has been an increase in violent attacks all over the world, including the World Trade Center attack in 2001. In response, there has been a heightened awareness of physical security needs the need to police the space around buildings, to control access to buildings, to design sound policies for evacuation in the event of a disaster, and to develop stronger points of contact with the local and federal authorities. On the technological front, there is a corresponding need to survey the threats to computing equipment (hardware), the applications and databases that reside on that equipment (software), and the networks that connect groups, both internally and with the outside world. In a business environment, raw data such as customer records or credit card information are valuable to competitors and computer criminals and require special attention. In addition, for more advanced enterprises, intellectual property including scientific research or unique business processes have high value and also require special security measures. As the world becomes an increasingly competitive place, the theft of both raw data and intellectual property assets via computer is on the rise. A combination of preventive maintenance supported in attitude and investment by the executive team, employee training and vigilance, and clear communications throughout the organization will help reduce the threats of physical and cyber security breaches.

The information needed to answer these questions will be found through conversations with employees (especially the IT staff), managers, and executives of the company. It will be useful to evaluate customer and supplier feedback on other issues as this may lead to revelations on security issues. Finally, the team gathering the information should be familiar with media reports about the company. Public perceptions may also be instructive, especially if the company is involved in a controversial industry, is located near a hot spot of activity, or has appeared in prominent publications on a regul

The first step in improving the security of your system is to answer these basic questions:

- What am I trying to protect and how much is it worth to me?
- What do I need to protect against?
- How much time, effort, and money am I willing to expend to obtain adequate protection?

These questions form the basis of the process known as *risk assessment*. Risk assessment is a very important part of the computer security process. You cannot formulate protections if you do not know what you are protecting and what you are protecting those things against! After you know your risks, you can then plan the policies and techniques that you need to implement to reduce those risks. For example, if there is a risk of a power failure and if availability of your equipment is important to you, you can reduce this risk by installing an uninterruptible power supply (UPS).

Risk assessments involves three key steps:

1) identifying assets and their value;
2) identifying threats;
3) calculating risks.

There are many ways to go about this process. One method with which we have had great success is a series of in-house workshops. Invite a broad cross-section of knowledgeable users, managers, and executives from throughout your organization.

Over the course of a series of meetings, compose your lists of assets and threats. Not only does this process help to build a more complete set of lists, it also helps to increase awareness of security in everyone who attends. An actuarial approach is more complex than necessary for protecting a home computer system or very small company. Likewise, the procedures that we present here are insufficient for a large company, a government agency, or a major university. In cases such as these, many companies turn to outside consulting firm with expertise in risk assessment, some of which use specialized software to do assessments.

III. 1. Identifying assets

Draw up a list of items you need to protect. This list should be based on your business plan and common sense. The process may require knowledge of applicable law, a complete understanding of your facilities, and knowledge of your insurance coverage. Items to protect include tangibles (disk drives, monitors, network cables, backup media, manuals) and intangibles (ability to continue processing, your customer list, public image, reputation in your industry, access to your computer, your system's *root* password). The list should include everything that you consider of value. To determine if something is valuable, consider what the loss or damage of the item might be in terms of lost revenue, lost time, or the cost of repair or replacement.

III. 2. Identifying threats

The next step is to determine a list of threats to your assets. Some of these threats will be environmental, and include fire, earthquake, explosion, and flood. They should also include very rare but possible events such as building structural failure, or discovery of asbestos in your computer room that requires you to vacate the building for a prolonged time. Other threats come from personnel, and from outsiders.

III. 3. Review risks

Risk assessment should not be done only once and then forgotten. Instead, you should update your assessment periodically, at least once a year, and any time there is a major change in personnel, systems, or the operating environment.*53* In addition, the threat assessment portion should be redone whenever you have a significant change in operation or structure. Thus, if you reorganize, move to a new building, switch vendors, or undergo other major changes, you should reassess the threats and potential losses.

III.4. Loss analysis

Determining the cost of losses can be very difficult. A simple cost calculation considers the cost of repairing or replacing a particular item. A more sophisticated cost calculation can consider the cost of having equipment out of service, the cost of added training, the cost of additional procedures resulting from a loss, the cost to a company's reputation, and even the cost to a company's clients. Generally speaking, including more factors in your cost calculation will increase your effort, but will also increase the accuracy of your calculations. For most purposes, you do not need to assign an exact value to each possible risk. Normally, assigning a cost range to each item is sufficient. Some items may actually fall into the category irreparable or irreplaceable; these could include loss of your entire accounts-due database, or the death of a key employee. You may want to assign these costs based on a finer scale of loss than simply "lost/not lost." For instance, you might want to assign separate costs for each of the following categories:

- non-availability over a short term (< 7-10 days);
- non-availability over a medium term (1-2 weeks);
- non-availability over a long term (more than 2 weeks);
- permanent loss or destruction;
- accidental partial loss or damage;
- deliberate partial loss or damage;
- unauthorized disclosure within the organization;
- unauthorized disclosure to some outsiders;
- unauthorized full disclosure to outsiders, competitors, and the press;
- replacement or recovery cost.

III.5. The probability of a loss

After you have identified the threats, you need to estimate the likelihood of each occurring. These threats may be easiest to estimate on a year-by-year basis. Quantifying the threat of a risk is hard work. You can obtain some estimates from third parties, such as insurance companies. If the event happens on a regular basis, you can estimate it based on your records. Industry organizations may have collected statistics or published reports. You can also base your estimates on educated guesses extrapolated from past experience.

III. 6. The cost of prevention

Finally, you need to calculate the cost of preventing each kind of loss. For instance, the cost to recover from a momentary power failure is probably only that of personnel "downtime" and the time necessary to reboot. However, the cost of prevention may be that of buying and installing a UPS system. Costs need to be amortized over the expected lifetime of your approaches, as appropriate. Deriving these costs may reveal secondary costs and credits that should also be factored in. For instance, installing a better fire-suppression system may result in a yearly decrease in your fire insurance premiums and give you a tax benefit for capital depreciation. But spending money on a fire-suppression system means that the money is not available for other purposes, such as increased employee training or even investments.

III.7. Adding up the numbers

At the conclusion of this exercise, you should have a multidimensional table consisting of assets, risks, and possible losses. For each loss, you should know its probability, the predicted loss, and the amount of money required to defend against the loss. If you are very precise, you will also have a probability that your defense will prove inadequate. The process of determining if each defense should or should not be employed is now straightforward. You do this by multiplying each expected loss by the probability of its occurring as a result of each threat. Sort these in descending order, and compare each cost of occurrence to its cost of defense. This comparison results in a prioritized list of things you should address. The list may be surprising. Your goal should be to avoid expensive, probable losses, before worrying about less likely, low-damage threats. *In many environments, fire and loss of key personnel are much more likely to occur, and are more damaging than a break in over the network.* Surprisingly, however, it is break-ins that seem to occupy the attention and budget of most managers. This practice is simply not cost-effective, nor does it provide the highest levels of trust in your overall system. To figure out what you should do, take the figures that you have gathered for avoidance and recovery to determine how best

to address your high-priority items. The way to do this is to add the cost of recovery to the expected average loss, and multiply that by the probability of occurrence. Then, compare the final product with the yearly cost of avoidance. If the cost of avoidance is lower than the risk you are defending against, you would be advised to invest in the avoidance strategy if you have sufficient financial resources. If the cost of avoidance is higher than the risk that you are defending against, then consider doing nothing until after other threats have been dealt with.

IV. Planning bank information security

This chapter covers policy and procedural issue related to creating an effective defense to the security threats presented in the previous chapter and goes into greater detail on the planning process. Thus, practical security is really a question of management and administration more than it is one of technical skill. Consequently, security must be a priority of your organization's management. Even in a very small enterprise without a significant budget for security, the management should understand the core security issues and implement basic (and relatively inexpensive) measures to protect its assets.

Security planning may be divided into five discrete steps:

1) Planning to address your security needs;
2) Conducting a risk assessment or adopting best practices;
3) Creating policies to reflect your needs;
4) Implementing security;
5) Performing audit and incident response.

Within this broad definition, there are many different types of security that both users and administrators of computer systems need to be concerned about:

IV. 1. Confidentiality

Protecting information from being read or copied by anyone who has not been explicitly authorized by the owner of that information. This type of security includes not only protecting the information *in toto*, but also protecting individual pieces of information that may seem harmless by themselves but that can be used to infer other confidential information [3].

IV. 2. Data integrity

Protecting information (including programs) from being deleted or altered in any way without the permission of the owner of that information. Information to be protected also includes items such as accounting records, backup tapes, file creation times, and documentation.

IV. 3. Availability

Protecting your services so they're not degraded or made unavailable (crashed) without authorization. If the systems or data are unavailable when an authorized user needs them, the result can be as bad as having the information that resides on the system deleted.

IV. 4. Consistency

Making sure that the system behaves as expected by the authorized users. If software or hardware suddenly starts behaving radically differently from the way it used to

behave, especially after an upgrade or a bug fix, a disaster could occur. Imagine if your ls command occasionally deleted files instead of listing them! This type of security can also be considered as ensuring the *correctness* of the data and software you use.

IV. 5. Control

Regulating access to your system. If unknown and unauthorized individuals (or software) are found on your system, they can create a big problem. You must worry about how they got in, what they might have done, and who or what else has also accessed your system. Recovering from such episodes can require considerable time and expense for rebuilding and reinstalling your system, and verifying that nothing important has been changed or disclosed—even if nothing actually happened.

IV. 6. Audit

As well as worrying about unauthorized users, authorized users sometimes make mistakes, or even commit malicious acts. In such cases, you need to determine what was done, by whom, and what was affected. The only sure way to achieve these results is by having some incorruptible record of activity on your system that positively identifies the actors and actions involved. In some critical applications, the audit trail may be extensive enough to allow "undo" operations to help restore the system to a correct state. Although all of these aspects of security are important, different organizations will view each with a different amount of importance. This variance is because different organizations have different security concerns, and must set their priorities and policies accordingly.

V. Conclusion

Fundamentally, computer security is a series of technical solutions to non-technical problems. You can spend an unlimited amount of time, money, and effort on computer security, but you will never quite solve the problem of accidental data loss or intentional disruption of your activities. Given the right set of circumstances – software bugs, accidents, mistakes, bad luck, bad weather, or a sufficiently motivated and well-equipped attacker – any computer can be compromised, rendered useless, or even totally destroyed. The job of the security professional is to help organizations decide how much time and money need to be spent on security. Another part of that job is to make sure that organizations have policies, guidelines, and procedures in place so that the money spent is spent well. And finally, the professional needs to audit the system to ensure that the appropriate controls are implemented correctly to achieve the policy's goals.

References

1. Guerra, Robert. The Right to Communicate. Ottawa, 2003.
   http://www.undp.org
2. FIL-69-2001. Authentication in an Electronic Banking Environment. 2001.
   http://www.worldbank.org
3. Thacker, K. IT Security Evaluation, CESG – United Kingdom, 2003.
   http://www.cesg.gov.uk/
4. Yusuf Musaji. A Definition of IT Security. ISACA, 2006.
   http://www.isaca.org/cobit.htm