Information Security Risk in Financial Institutions

James A. Nelson

***Abstract*—**The history of technology and banking is examined as it relates to risk and technological determinism. It is proposed that the services that banks offer are determined by technology and that banks must adopt new technologies to be competitive. The adoption of technologies paradoxically forces the adoption of other new technologies to protect the bank from the increased risk of technology. This cycle will lead to bank examiners and regulators to focus on human behavior, not on the ever changing technology.

***Keywords*—**Banking, information security, risk, technological determinism.

I. Introduction

FINANCIAL Institutions in the United States are regulated by Federal and State Governments and undergo almost continuous examination for compliance with law. The purpose of the law and these examinations is to protect the banking consumer from fraud and unauthorized disclosure of non-public information. Until recently these examinations have targeted banking technologies and the procedures and policies that accompany the technologies.

The examiners concern with information technology was directed at the accuracy and reliability of the systems that processed the institutions transactions. The computer system itself was considered as a source of risk because of relatively high probabilities of failure inherent in the hardware and software. Human error in following procedures and data entry was also a major area of concern.

Regulators examined input/output controls, reviewed data sets, and tested extreme values. If the information technology system generated accurate output, the system was considered as low risk. Check sums, accounting accuracies, and dual control procedures for human access to system change values were the focus of regulator attention.

With the evolution of banking computer systems from centralized mainframe technologies with terminal input/output, risk increased moderately as more employees had access to the system. Controls were still primarily accounting controls and the lack of knowledge of most employees about esoteric computer hardware and software (ignorance as a control). With the advent of personal computers and the replacement of terminal based systems with local area networks using internal communication systems, risk increased as more employees had access to the system. Systems became easier to use and computer skills became more common place in the culture. At this stage all systems are still internal to the bank, and risk is mitigated by due diligence in selecting employees and monitoring accounting systems.

Even with the widespread introduction of branch banking via common carrier communication systems, the core banking system was at low risk of intrusion by bank outsiders because the network was relatively private. Then came the Internet and suddenly financial institutions were vulnerable to attacks not only from people physically inside the bank, but from anyone with an Internet connection anywhere in the world.

The primary concern of both bankers and regulators became hacking. With the rapid adoption of new technologies as a necessity for competitive advantage for financial institutions, technology became the focus of regulator's efforts to combat hacking. Banks began to use stronger access controls, firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), encryption, two-factor authentication, and other controls and mitigating strategies to protect their most valuable asset – information. Hackers also took advantage of the rapid changes in technology to exploit weaknesses in the financial computing systems.

Technologies were seen as the focus of competition and paradoxically the source of risk and the control of risk. As banking technologies change, technological solutions to the increased risk have also changed. The attack strategies, sophistication of techniques, and the opportunities for hackers have increased dramatically as banking technologies have embraced the Internet.

II. Technological Determinism

Technology will continue to change and hackers will continue to hack. Banks adopt the latest technologies to provide their customers with competitive services. As they adopt new technologically based services they must also adopt new protective technologies or they will increase their risk to hacking. A bank can never say "Enough! We don't need more technology". To do so would be to admit defeat from two directions: failure to adopt new technologies would decrease the bank's competitiveness for customers and at the same time

Manuscript received November 14, 2005.

James A. Nelson is with the Department of Accounting & Information Systems, College of Business, New Mexico State University, Las Cruces, NM 88003 USA (phone: 505-646-5678; fax: 505-646-1552; e-mail: jnelson@nmsu.edu).

open the vaults to those that found new technological keys.

The term "technological determinism" is widely attributed to the American sociologist and economist Thorstein Veblen early in the 20th century. In considering technology, Veblen stated that "The factor in the modern situation that is alien to the ancient regime is the machine technology, with its many and wide ramifications".

Chandler [1] provides a summary of social scientists and communications theorists' use of technological determinism to refer to the assumption that new technologies are the determining cause of major social and historical changes. Extreme technological determinists hold that technology will radically transform the world and how humans behave and think. Chandler describes how this view "enrages modern sociologists" who hold that technologies are subordinate to the socio-cultural environment. The Canadian communications theorist, Marshall McLuhan, was the most popular proponent of the power of technology in determining culture and the content of our lives. McLuhan's famous phrase "the medium is the message" reflects technological determinism's assumption that technology is the means and the meaning of communication.

III. Technological Determinism in Banking

Technological determinism has been widely debated in sociology and communications studies, but has received little attention from the technological and business communities. A paper by Nelson [2] introduced the concept of technological determinism in the banking industry years the explosion of technological and Internet based banking services. Nelson stated that new technologies will determine the competitive behavior of banks. Banks must adopt technologies to survive. Banks don't have a choice; customers will demand the latest technologies of Internet banking, bill pay, ATMs, smart cards, voice response systems, cell phone banking, and unknown future systems. In a reaction to banking technologies, some banks will use "personal banking", but this non-technical approach will be a reaction to technology and thus determined by technology. Even personal banking is technologically driven and assisted by technology.

This work was done in the 1980's before the advent of Internet banking and failed to foresee that technology would also determine the risk mitigation and control strategies that banks would adopt in the late 20th and early 21st centuries. Today, technology not only determines what services and products a bank offers, but that the adoption of competitive technologies also determines the nature of banking risks. Technology determines the risks and dictates that more technologies will be used to mitigate and control the risk.

If banks don't adopt new defensive technologies they will increase their risk by default, because hackers will always use the latest technologies to their advantage.

Technology is the driving force in banking. Technology determines what services will be offered and technology is used to protect the bank from threats that would not exist if it were not for the services offered.

IV. Banking and Regulatory Exams

Because technologies change so rapidly and so many technologically based products and services are used and offered by banks, it becomes a formidable task for regulators to understand the technologies they are examining. Examiners pass judgment on technological risks that they neither understand nor have the time to evaluate. As exams became more technical neither the examiners in the field nor the bank officers are capable of any response other than "Buy new technological controls". Regulators all too easily get caught up in the cycle of requiring new technologies to control technologies, which then requires newer technologies to manage the increased risk.

The behavior of regulators and their exams has been determined by the technologies that are used by banks for competitive reasons and by technologies that are used to protect those very technologically based services. The cycle of technological adoption and increasing sophistication has made it impossible for regulators to maintain control over the technology.

In an attempt to reduce technologically based risk, banks are removing access to powerful technologies. This demonstrates a basic truth: technology is not a threat; humans using technologies are the threat. The power of desktop PCs has dramatically increased the threat that each user poses to the bank. Desktop PCs, which are designed to add value to the work that each individual banker performs, can also be the source of malevolent programs and access. These programs can be either the result of external hacking or both intentional and intentional behavior on the part of the banker. The current trend in financial institutions is to reduce risk by decreasing the range of system and user applications that are available at the desktop. "Thin clients", which are nothing more than a supercharged version of the terminals of yesteryear, allow powerful banking applications to be executed by the user. The value of thin clients lies in the increased centralized control and the corresponding decrease in the number of machines that could potentially harbor threats. Access to the systems resources by external and internal persons is severely limited. Here we see that although technology is increasing its power, the controls are designed to manage and limit human involvement with the technologies.

Bankers and regulators are both realizing that the real threat is not the technology, but the humans that use the technology. Human users are the source of errors, defalcations, and information theft. Technologies will always change, but the behavior of humans remains relatively constant. We make errors, we steal, and we do good. Examiners are dramatically changing the focus of the exams from technology to people. People will take whatever technology is current and use it for good or evil. Our job as bankers, auditors, and examiners is to ensure that the technologies are managed. In the future, exams will not be a review of the banking technologies and their technological controls, but on the bank's management policies, practices, and procedures. To ensure that the focus is

not on the never ending change in technologies, the reviews will focus on those individuals most likely to have the least technological expertise – management. The Boards of Directors will be held responsible and examined on the policies, practices, and procedures used for the management of technologies for which they have little understanding.

Examiners and bankers cannot be expected to understand the physics, engineering, and computer science that is ever changing and evolving, but they are responsible for its implementation and proper use. Directors will be "responsible for verification and assurance of practices and controls on management through audit and independent review programs" [3]. Regulators have stopped chasing technologies. They know that technology will always change, that hackers will always hack, and that as examiners they do not and cannot compete at the level of technology. All they can do is ensure that policies, procedures, and practices are in place to manage the unmanageable – technology.

REFERENCES

[1] D. Chandler, "Engagement with media: Shaping and being shaped," *Computer-Mediated Communication Magazine*, February, 1996. Available: http://www.december.com/cmc/mag/1996/feb/chandler.html

[2] James A. Nelson, "A technologically determined model of the financial services industry," presented at the 1986 Western Academy of Management, Reno, NV.

[3] FDIC, 2005