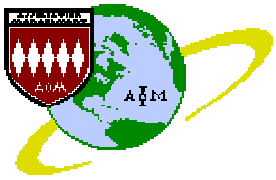

Journal of Information Technology Management

ISSN #1042-1319

A Publication of the Association of Management

THE CEO'S VIEW OF THE IMPACT OF IT SECURITY REQUIREMENTS WITHIN CREDIT UNIONS

JAMES D. HARRIS
Pittsburg State University
jdharris@pittstate.edu

FELIX F. DREHER
Pittsburg State University
ffdreher@pittstate.edu

MAEVE L. CUMMINGS
Pittsburg State University
cummings@pittstate.edu

ABSTRACT

The goals for this study are to better understand how credit unions and their management teams cope with issues surrounding information assurance and computer security. Credit union CEOs in seven Midwestern states were surveyed to gain insight into the impact that computer security and information assurance requirements are having on credit unions and their management teams. The survey included questions addressing the credit union size, information system infrastructure, and computer related services provided. Survey questions also addressed major concerns, policy issues, impact on the management team and the board of directors, training, reviews, and other related topics. Survey results show that credit union CEOs understand the requirements for appropriate IT security; however, meeting evolving requirements in this area is a challenge and some areas such as employee training may need to be enhanced.

Keywords: Information Assurance, computer security, credit unions

INTRODUCTION

The goals for this study are to better understand how credit unions and their management teams cope with issues surrounding information assurance and computer security and from this understanding to derive implications for information systems curricula. Credit unions are impacted by the issues surrounding IT security in much the same way as other organizations. Those issues relate to the ramifications associated with ensuring confidentiality, integrity, and availability of customer information. To remain competitive, credit unions are relying more extensively on information technology and are providing their customers with a wider variety of on-line services. This increased reliance on information technology and the evolving legal and regulatory environment provide new challenges to credit union management teams and their boards of directors. Laws such as the Gramm-Leach-Bliley Financial Services Modernization Act [1] address security obligations that financial services organizations must satisfy. The National Credit Union Administration (NCUA) provides

standards that reflect the legal obligations spelled out in Gramm-Leach-Bliley. In particular, the NCUA Guidelines for Safeguarding Member Information require the development of a comprehensive information security program which must be approved, supervised, and monitored by the credit union board of directors. The information security program must address assessment, management, and control of security risks. The credit union must also ensure that appropriate controls are used to insure the confidentiality and integrity of member information and the transactions that use that information. There are also obligations related to monitoring network access and responding to perceived attacks, providing appropriate staff training, and testing key procedures and controls. [4]

Like many small businesses, the small to medium size credit unions do not have extensive financial and staff resources that can be dedicated to the development and implementation of information security procedures and controls. As a result they often rely on guidance from national organizations along with suggestions from equipment and software vendors. Developing the policies and controls and acquiring the hardware and software necessary to implement those policies and controls is only the beginning. The majority of the cost, along with many of the major challenges, are related to "configuration, maintenance, and the subsequent monitoring, reporting, and analysis of generated logs and alerts." [3] As a result, many financial services organizations are contracting with a managed security service provider (MSSP) to provide the technical support needed to manage security controls. The MSSP will have trained security staff available 24/7 to insure that security controls are consistently applied and attacks are identified and responded to in an appropriate manner.

TYPICAL CREDIT UNION ORGANIZATION

Credit Union policies and procedures are the responsibility of three distinct groups of individuals: the Board of Directors, the Supervisory Committee, and the Management Team. The Board of Directors is elected by the membership of the Credit Union and is responsible for overseeing the operation of the credit union. The Board of Directors is the chief planning and policy-setting group. The Supervisory Committee is responsible for overseeing the financial soundness of the Credit Union and arranges for audits of the financial records and policies of the Credit Union. Most supervisory committees will engage an external audit firm to conduct audit reviews. The supervisory committee will also meet with state or federal examiners to discuss the results of their reviews. Finally, the management team is responsible for implementing the policies and procedures approved by the Board of Directors. The management team does day-to-day supervision of CU activities, reports to Board on regular basis, and is responsible for employee training and supervision. As such they are responsible for ensuring that policies are known by employees and that procedures are in place to protect the resources of the Credit Union.

As Federal or State Chartered Financial institutions, the policies and procedures of the Credit Union are periodically reviewed by the state and federal examiners. Reports of these examinations are provided to the Board of Directors, the Supervisory Committee, and the Management team.

SURVEY PURPOSE AND STRUCTURE

Credit union CEOs in seven Midwestern states were surveyed to gain insight into the impact that computer security and information assurance requirements are having on credit unions and their management teams. The survey included questions addressing the credit union size, information system infrastructure, and computer related services provided. Survey questions also addressed major concerns, policy issues, impact on the management team and the board of directors, training, reviews, and other related topics.

The target population was Federally Insured Credit Unions with assets exceeding 10 million dollars and which are located in one of seven Midwestern states. A total of 239 credit unions were selected from Kansas, Oklahoma, Nebraska, North Dakota, South Dakota, Idaho, and Wyoming. The National Credit Union Administration (NCUA) supervises federal credit unions and insures savings in federal and most state-chartered credit unions across the country through the National Credit Union Share Insurance Fund (NCUSIF), a federal fund backed by the full faith and credit of the United States government. NCUA is also the source of regulations related to many operational issues for both Federal and State charted credit unions. Of the 239 surveys distributed 56 completed surveys were returned. This represents a 23.4% return rate. The survey was addressed to the Chief Operating Officer as listed in the NCUA Directory of Federally Insured credit unions.

SURVEY RESULTS

The first survey section asked about the current services and future plans in nine different areas. The responses documented in Table 1 show that Funds Transfers and internal processing of transactions will be used by over 80 percent of the respondents within the next three years. In-house support for ATM's will be provided by less than 40% of the respondents and approximately 43% of the respondents will be using an external service bureau to provide all services. The greatest planned service changes over the next three years were related to increased utilization of external service bureaus and the provision of in-house support for Internet based account transactions.

Table 1
IT Services Provided

	Current services	Planned future services	Total	% total credit unions surveyed
Electronic transfer of funds, check clearing, etc.	42	3	45	80.36%
In-house processing of transactions and records	34	1	35	62.50%
In-house support for loan applications and loan processing	34	5	39	69.64%
In-house support for Credit or Debit Cards	27	4	31	55.36%
In-house support for Internet account inquiries	25	5	30	53.57%
We use an external service bureau to provide some of our services	25	9	34	60.71%
In-house support for Internet based account transactions	24	8	32	57.14%
In-house support of ATM's	17	5	22	39.29%
We use an external service bureau to provide all of our services	15	9	24	42.86%

Seventy-five percent of the surveyed credit unions have at least one officer with specific responsibilities for planning, oversight, and operational management of the computer information services. The names provided for the officer with this responsibility included: President, Manager, or CEO (18); VP of Finance, CFO (5); Other Vice-President (9); and IS Coordinator, IS Manager, System Administrator, Technical Manager (11). When ask about the sources of support for the IT operations the respondents indicated that 53.2% of the support for their computer information infrastructure comes from vendors, 33.1% of the support is provided in-house, 9.8% of the support comes from consultants, and 3.9% of the support comes from other sources.

To get a handle on some of the traditional issues related to privacy, security, employee responsibilities, institutional policies, and other non-technical issues the survey included a set of questions that addressing policy and procedural issues. For these questions the respondent was asked to indicate their degree of agreement using a 5-point scale. The scale ranged from 1 to 5 with 1=Strongly Disagree, 2=Disagree, 3=Neutral, 4= Agree, and 5=Strongly Agree.

The first of these sets of survey questions dealt with policy issues and the impact that these issues have on employees, the Board of Directors, and the Supervisory Committee. The mean and standard deviation for the responses to these questions is given in Table 2.

Table 2:
Management Policy Issues

Question	x	s
Policies that define the responsibilities of employees regarding the need to protect privacy and security of member records are required by State and Federal Credit Union Regulation.	4.70	0.54
We believe we have developed and have in place comprehensive policies to control the way we manage, protect and allocate information resources.	3.86	0.64
We have reviewed all of our policies and procedures related to computer security and information assurance within the past two years.	4.27	0.75
We believe that we have developed verification procedures, which insure that all policies related to computer security and information assurance are followed.	3.79	0.82
Our employees are well trained regarding our policies and procedures related to computer security and information assurance.	3.64	0.75
We ensure that our policies and procedures are followed by using reviews, examinations, and testing.	3.57	0.78
The Supervisory committee should review policies related to use of Information Technology as part of their role within the Credit Union	3.86	0.9
The supervisory committee is involved in procedures that check to see that policies related to use of Information technology are being followed.	2.84	1.09
The Board of Directors regularly reviews policies related to the use of Information Technology as part of their role within the Credit Union	3.79	0.87
We have a process in which management formally accepts the adequacy of each new computer system's security provisions.	2.95	1.00

There is a very high level of agreement (mean 4.70) that State and Federal Credit Union regulations require policies that define the responsibilities of employees for the protection of privacy and security of member records. Agreement with the statement that comprehensive policies have been developed to control the management, protection, and allocation of information resources is somewhat lower (mean 3.86). Most credit unions have recently reviewed their computer security and information assurance policies (mean 4.27).

Agreement with the statement that the supervisory committee is involved in the verification that information technology policies are being followed was the lowest in this section (mean 2.84). There was a higher level of agreement that the supervisory committee should be involved in such reviews (mean 3.86) and there was a fairly high level of agreement that the Board of Directors is actually involved in these reviews (mean 3.79). Since agreement with the statement that comprehensive policies controlling the management, protection, and allocation of information resources have been developed had a mean of 3.86, it seems reasonable that existence of associated verification procedures (mean 3.79) and employee training regarding such policies (mean 3.64) would have similar or somewhat lower means. The response was fairly neutral (mean 2.95) to the question "We have a process in which management formally accepts the adequacy of each new computer system's security provisions." This would seem to indicate that many credit unions have not implemented such a process. Such a process would allow management to verify that the level of protection and risks associated with a new system are well understood before that system is placed in production use. [2]

A second section of the survey included several questions relating to the respondent's perception of the importance to members of the confidentiality and integrity of computerized records. This section also included several questions relating to the responsibilities of employees and the Board of Directors. The means and standard deviations of the responses are given in Table 3.

Table 3
Members Interests and Employee Responsibilities

Question	x	s
The confidentiality of computerized records is of extreme importance to our members.	4.79	0.56
It is of extreme importance to our members that all records, especially our computerized records are always accurate and that they are used only for authorized purposes.	4.88	0.33
Our employees are aware of the State and Federal laws which require that we provide adequate security for any member's records that we retain in a computer system, transmit over a network, or use in our operations.	4.38	0.62
The Board of Directors expects that the management team will conduct reviews of our institution's computer system's security procedures on a regular basis.	4.46	0.69
The policies for insuring the privacy and security of computer records are currently being reviewed more intensively by the external auditors than in previous years.	4.21	0.87

It is apparent that the respondents strongly agree that confidentiality and integrity of computerized records is highly important to credit union members. The respondents feel that their employees are aware of related State and Federal laws (mean 4.38). There is also agreement that the Board of Directors expects the management team to conduct regular reviews computer system security procedures (mean 4.46). Also, policies related to privacy and security of computer records are being reviewed more intensively by external auditors (mean 4.21).

A third set of the questions dealt with concerns and threats related to computer security and information assurance and the possible limiting effects that those concerns might have on the utilization of information technology. The mean and standard deviation of the responses to these questions is given in the Table 4.

Table 4
Computer Security and Information Assurance Threats

Question	x	s
Improper use of personal and financial data by employees is not a major concern.	2.86	1.34
Viruses, Worms, and other malicious software are more of an operational problem than a threat to the data we maintain in computer systems.	2.68	1.27
We invest more resources in providing backup and recovery from disasters such as fire, wind damage, or computer failure than any other type of threat.	3.36	1.00
We are more concerned with the physical security of the data stored in our computer systems than we are with its theft or destruction due to computer hackers.	2.80	1.07
Our telecommunication resources are secure since we only use dedicated or dial-up communications supplied by a telecommunications services company.	2.63	1.24
We do not currently have a Web based system since we are concerned about the impact of such a system on the security of our information.	2.02	1.07
The use of Virtual Private Networks and Secure Transactions using encryption techniques will allow access to Web based systems with minimal threat to our customer information.	3.46	1.01
We anticipate that we will need to invest a significant amount of resources in the next two years to meet the threats presented by computer hackers, viruses, etc.	3.54	0.87

The respondents tended to disagree (mean 2.02) with the statement "We do not currently have a Web based system since we are concerned about the impact of such a system on the security of our information." This response is consistent with the current and planned support for Internet based account transactions reported in Table 2. The other statements in this section elicited fairly neutral responses ranging from a mean of 2.63 to a mean of 3.54. This may indicate a balanced view of the threat landscape with computer security and information assurance threats being considered of equal but not greater gravity than other types of threats and responsibilities that the credit union must address. The neutral response(mean 2.86) to the statement "Improper use of personal and financial data by employees is not a major concern." could indicate a high level of confidence

in the integrity of employees and existing safeguards or it could indicate some lack of appreciation for the potential seriousness of this concern.

A fourth set of questions addresses the sources for information regarding threats and fixes or protection against them. The mean and standard deviation of the responses to these questions is given in Table 5.

Table 5
Sources of Information Regarding Threats

Question	x	s
We can depend upon our computer systems vendors for timely information related to threats and fixes for computer security issues.	3.75	0.86
We can depend upon our external auditors for timely information related to threats and fixes for computer security issues.	2.91	1.05
We can depend upon the state and federal regulator agencies for timely information related to threats and fixes for computer security issues.	3.00	1.01
We can depend upon the state credit union association for practical procedures and policies related to computer security and privacy issues.	2.71	1.41
We really do not have any single source where we can find the critical information required to meet our needs in the area of computer security and privacy.	3.45	1.17

The above responses show that vendors are depended on more heavily for information regarding threats and protection (mean 3.75) than are external auditors (mean 2.91), regulatory agencies (mean 3.00), or state credit union associations (mean 2.71). This dependence of vendors for information regarding threats and the associated fixes is not surprising since as previously noted, credit unions depend heavily on vendors to support their information technology infrastructure. There was some agreement that there is no single source providing this information (mean 3.45).

CONCLUSIONS

To remain competitive credit unions are offering more services that depend on information technology. While these services may expose the organization to new threats to the confidentiality and integrity of member information, the risk that these threats will be exploited is not sufficient to deter the credit unions from offering these new services. This suggests that risk management is an essential process for CEOs to implement within their organization.

The credit union CEO's who responded certainly appreciated member interest in the confidentiality (mean 4.79) and accuracy (mean 4.88) of computerized records. Survey respondents also indicated that they have developed comprehensive policies regarding information resources (mean 3.86), that they verify that those policies are followed (mean 3.79), that the Board of Directors regularly reviews those policies (mean 3.79), and that the supervisory committee should review those policies (mean 3.86). Although these responses indicate general agreement in each of these areas, a higher level of agreement might be expected since there is an NCUA guideline suggesting that the information security program be approved, supervised, and monitored by the credit union board of directors.

Policy development, policy enforcement, verification of adherence to policies, and employee training regarding policies are critical issues which have legal and ethical implications for most organizations. Respondents agree that policies defining the responsibilities of employees to protect privacy and security of member records are required by law (mean 4.70), that employees are aware of such laws (mean 4.38), and that employees are well trained regarding related policies and procedures (mean 3.64). Since employee training is also an NCUA guideline there appears to be a need for more focus on employee training especially related to policies and procedures.

Policies for insuring privacy and security of computer records are being reviewed more intensively by external auditors than in previous years (mean 4.21) and such policies have been reviewed internally within the past two years (mean 4.27).

Since vendors have a vested interest in the products they supply it is of some concern that respondents seem to rely more heavily on vendors for timely information related to threats and fixes for computer security issues. A related concern is that respondents agreed with the statement that they do not have any single source to find critical information required to meet there needs in the area of computer security and privacy (mean 3.45). There may be a need for professional societies and regulatory agencies to work harder to provide this information in a form that is

accessible to small and medium size credit unions. This reliance on vendors suggests that information technology leaders within the organization be provided with training that addresses the development and supervision of vendor contracts.

It is likely that the person with specific responsibilities for planning, oversight, and operational management of the computer information services will hold a position such as CEO, CFO, or Vice President rather than a more technically oriented position such as system administrator or IS manager. Since information assurance and computer security concerns have grown rapidly in recent years the security posture of the organization could potentially be enhanced by providing key leaders with training regarding relevant threats to information resources along with appropriate countermeasures.

REFERENCES

[1] Gramm-Leach-Bliley Financial services modernization act, Banking.senate.gov/conf/grmleach.htm, retrieved November 22, 2004.

[2] Harris, S., *All-In-One CISSP Certification*, New York, New York: McGraw Hill, 2003.

[3] Levine, Lawrence, Cost-justifying managed security for financial institutions, *Community banker.* March, 2004.

[4] National Credit Union Administration, Guidelines for safeguarding member information, http://www.ffiec.gov/exam/InfoBase/documents/02-ncu-12_cfr_748_app_a_safeguard_info-010100.pdf, retrieved November 22, 2004.

AUTHOR'S BIOGRAPHIES

James Harris is University Professor of Computer Science and Information Systems at Pittsburg State University. He holds the Ph.D. degree from the University of Virginia as well as the CISSP, MCSE, Network+, and IAM certifications. Dr. Harris teaches courses in information assurance and computer security, computer networks, software engineering, programming languages, and C++ programming. His recent publications have related to software engineering education, computer ethics and information assurance education.

Felix Dreher is an Associate Professor and Chairperson in the Department of Computer Science-Information Systems at Pittsburg State University. He holds the Ph.D. degree from the University of Kansas and he teaches undergraduate level courses in digital logic, computer organization, computer architecture, operating systems, and systems administration. He maintains several small, dedicated computer laboratories that are used in the courses that he teaches as well as courses in computer networking and computer and network security. His research interests tend toward development of materials to support his teaching. He has also explored how to increase the role of in writing within computer science courses.

Maeve Cummings is Professor of Computer Science and Information Systems at Pittsburg State University. She holds the Ph.D. degree from the University of Texas at Arlington. Dr. Cummings teaches courses in computer applications, management information systems, COBOL, global information systems, and information assurance and computer security. She is author of a widely adopted management information systems textbook. Her current research interests are in the area of global information systems, security, and privacy.