



**An Information Systems
Security Readiness Assessment
for Municipalities in Rural Pennsylvania**

The Center for



Rural Pennsylvania

A Legislative Agency of the Pennsylvania General Assembly

An Information Systems Security Readiness Assessment for Municipalities in Rural Pennsylvania

By

**Jungwoo Ryoo, Ph.D., Tulay Girard, Ph.D., and Charlotte E. McConn, M.S., CDP.
Pennsylvania State University-Altoona**

November 2009

This project was sponsored by a grant from the Center for Rural Pennsylvania, a legislative agency of the Pennsylvania General Assembly.

The Center for Rural Pennsylvania is a bipartisan, bicameral legislative agency that serves as a resource for rural policy within the Pennsylvania General Assembly. It was created in 1987 under Act 16, the Rural Revitalization Act, to promote and sustain the vitality of Pennsylvania's rural and small communities.

Information contained in this report does not necessarily reflect the views of individual board members or the Center for Rural Pennsylvania. For more information, contact the Center for Rural Pennsylvania, 625 Forster St., Room 902, Harrisburg, PA 17120, telephone (717) 787-9555, email: info@rural.palegislature.us

EXECUTIVE SUMMARY

This research project, which is the first of its kind for local governments, assessed the information systems security readiness of municipalities in Pennsylvania, with an emphasis on rural municipalities.

The researchers developed a set of survey instruments that measured the following three major aspects of a municipality's information systems security readiness: (1) infrastructure, (2) computer literacy, and (3) daily practices.

Among the 276 municipalities statewide that participated in the study, 67 percent were rural and 33 percent were urban. The respondents included individuals representing Pennsylvania boroughs, townships and cities.

To assess the infrastructure of the participating municipalities, the researchers measured various criteria in the areas of hardware and software infrastructure, funding and human resources. From the evaluation, the researchers identified the following factors that may challenge the security readiness of rural municipalities:

- Lack of human resources: 81 percent of the rural municipal respondents had no dedicated in-house information technology (IT) support personnel, and only 46 percent outsourced their computer hardware/software support.
- Insufficient budget for improving information systems security: 25 percent of rural municipal respondents spent nothing on information systems security during the previous 5 years.
- Increased vulnerability as more municipal computers are connected to the Internet: on average, rural municipal respondents had three desktop computers connected to the Internet.

- Less than optimal installation of security software: a significant number of rural municipal respondents said they did not have any security software installed on their computers.

To assess computer literacy, the researchers measured various criteria in the areas of computer training and knowledge and security training and knowledge. From the evaluation, they identified the following factors as potential weaknesses of rural municipalities:

- Little computer training provided to the computer users.
- Little information systems security training provided to the computer users.
- Lack of security knowledge among users as almost one half of rural municipal respondents said their information systems security knowledge was below average.

Daily practices were assessed by measuring a whole host of criteria including computer sharing among employees, remotely accessing municipal computers, managing inventory, using various encryption methods, handling email, backing up and disposing of data, and disaster recovery. The researchers identified the following as potential weaknesses of rural municipalities:

- Lack of service agreements addressing security issues between municipalities and information technology contractors:

only 32 percent of rural municipal respondents had such agreements.

- Relaxed access control: 63 percent of rural respondents adopted improper user name/password practices, such as not using either a user name or password. Also, 64 percent of rural respondents were never asked to change their passwords.

Table of Contents

Introduction	4
Related research	5
Goals and Objectives	5
Infrastructure assessment	5
Computer literacy and security literacy assessment	5
Daily practices assessment	6
First of a kind research related to local government assessment	6
Methodology	6
Survey limitations	6
Results	7
Sample description	7
Infrastructure assessment	7
Computer literacy assessment	9
Security literacy assessment	10
Daily practices assessment	11
Conclusions	15
Policy Considerations	17
Local government action	17
State government action	17
Legislative support	17
Federal funding	18
References	19

- Unknown or no encryption used for a majority of municipal wireless local area networks.
- Inappropriate data backups: the municipalities backed up their data but did not verify it.
- Insufficient physical security: the municipalities had only a bare

minimum of physical security tools.

- Inadequate disposal of computers and other media containing sensitive information.
- Lack of security policies for a majority of municipalities.
- Loose network monitoring: 63 percent of rural respondents did not monitor the logs of network connection activities.

Based on the research findings, the researchers offered a variety of practice and policy considerations for both local governments and state government. These considerations include:

- Encouraging resource pooling among municipalities to share IT staff with security expertise;

- Encouraging periodic assessment of information systems security readiness among rural municipalities to monitor progress or any potential deterioration;
- Encouraging the development of written policies for enforcing sound, daily information systems security practices;
- Providing awareness training and security education for rural municipal employees;
- Providing a centralized incident management system that keeps track of security breaches and recognizes patterns, if any, that surface; and
- Developing a Web site that promotes community-driven exchanges of ideas and local-government-specific information systems security best practices.

INTRODUCTION

In 2006, a foreign attacker invaded computers at a water filtering plant near Harrisburg, Pa. According to press reports, the intruder installed malicious software that could have affected “the plant’s water treatment operation” (Esposito, 2006). In this particular case, an employee’s home computer, which had remote access to the water plant, was compromised.

In 2005, Russian hackers breached a Rhode Island government Web site and stole credit card information (Web Application Security Consortium, 2007).

In 2004, a Midwestern city police force lost its radio communications for five hours because of a virus on the city’s computer system (Krouk, 2004).

As these incidents indicate, computer crimes targeting local governments and computer security-related mishaps are not uncommon (Computer Security Institute, 2006; Web Application Security Consortium, 2007; Krouk, 2004). Rural municipalities may be particularly vulnerable because they typically lack necessary human and financial resources to adequately manage their information systems security.

The continuing push for e-government makes rural local governments even more vulnerable. E-government refers to the use of Information and Communication Technology (ICT) by government organizations to provide services to the general public, businesses, and other government organizations. Each day, more and more municipalities go online and provide their services via the Internet. In an ideal e-government scenario, information only would be available to individuals who need it and are authorized to access it. However, without careful planning and oversight, information can be abused easily and used against the interests of those it was intended to serve.

An online presence may pose other threats as well, especially when local governments host their own Web servers and allow other municipal computers to be part of the same network. When connected without proper security measures, these computers are potentially accessible to anyone on the Internet. With sufficient computer expertise and malicious intent, hackers can inflict serious damage.

Even without a direct Internet connection in their municipal offices, municipalities may be at risk because of widespread use of laptops and portable storage devices, such as USB drives. These devices make sensitive data more susceptible to loss, abuse and hacking attempts. Workplace laptops or portable storage devices are often connected to poorly guarded home networks of local government employees, which is as risky as the previous scenario in which office computers are networked to the Internet without adequate protection. Once plugged into inadequately protected home computers, portable storage devices may become another source of vulnerability. The data on them can now be stolen, damaged or changed by attackers. In addition, when the device is used again in the municipal office, malware from a home computer can infect the entire office network.

Outsourcing computer services can be another area of concern for some rural municipalities that hire consultants to install and manage computer hardware and software. There may be a tendency for municipalities to overlook whether necessary security precautions have been taken during the contract work. It is also common that consultants develop software or process data for the municipalities. In these situations, monetary constraints and a lack of expertise make it difficult for municipalities to test the software for

security and to check whether the data are securely handled during the outsourced processing.

The researchers' pilot study that laid the groundwork for this research project included interviews with officials at urban and rural municipalities in central Pennsylvania (McConn et al., 2007) and confirmed the concerns listed above. The researchers recognized the need for a comprehensive assessment to better understand the status quo of information systems security readiness in small rural municipalities.

This report describes the research conducted in 2008 to assess the level of security readiness in terms of hardware and software infrastructures, computer and security literacy, and daily information technology (IT) practices within Pennsylvania's municipalities. The researchers believe that the findings will eventually lead to concrete efforts at both the state and local government levels to prevent future computer security breaches.

Related research

A comprehensive literature review reveals that this research project is the first of its kind. Few studies have targeted rural local governments and scrutinized their information systems security readiness. No federal government agency has commissioned such research. Prior to this work, no state governments, including Pennsylvania, have commissioned such research, although some attempts have been made to

understand the degree of computer use among local governments (The Center for Rural Pennsylvania, 2005).

Realizing the lack of research in this area, the researchers conducted an exploratory study and published their initial findings in 2007 (McConn et al., 2007).

The Computer Security Institute (CSI), a professional society for serving the needs of computer security workers, has conducted studies that include local governments, but the number of respondents is very limited (4 percent in 2008). In addition, the surveys do not differentiate between urban and rural municipalities.

Most other assessment efforts have focused mainly on federal and state governments as demonstrated in the 2006 National Association of State Chief Information Officer (NASCIO) survey (NASCIO, 2006). The survey concentrated on measuring how the chief information officers of each state perceived the information systems security readiness of their state.

At the federal level, existing laws, rules, and regulations require government agencies to have IT security performance measurements regularly (Chew et al, 2006). These include the Clinger-Cohen Act, Government Performance and Result Act (GPRA), and Federal Information Security Management Act (FISMA).

GOALS AND OBJECTIVES

This research project assessed the information systems security readiness of rural municipal governments in Pennsylvania using the following evaluation criteria: hardware and software infrastructures, computer and security literacy, and the daily practices of using existing infrastructures and knowledge. These evaluation criteria allowed the researchers to quantify different aspects of security readiness.

Infrastructure assessment

The first objective was to investigate the software and hardware solutions rural municipalities use to: control both incoming and outgoing data traffic; encrypt and decrypt confidential information; limit access to computer systems and their resources; detect and remove malware including viruses, Spyware, Adware, worms, and Trojan horses; back up and restore data; and recover from disasters.

Computer literacy and security literacy assessment

The second objective was to measure both the computer literacy and security literacy of municipal employees. Computer literacy refers to how knowledgeable employees are about the municipality's information systems while security literacy refers to the level of computer-security-specific knowledge that each employee has in addition to computer literacy.

Rural local government workers were evaluated for the degree of their computer knowledge of: installing and configuring software and hardware; using software packages and hardware; installing, configuring and managing a network; and developing software.

For security literacy, municipal workers were evaluated for their knowledge of: security planning; the presence of internal threats, such as employees deleting important data, and external threats, such as hackers sending e-mails containing viruses and worms; security software and hardware features and their uses;

proper configuration and management of networks for improving security; methods to monitor suspicious activities on their computers; application of physical security principles, such as using computer locks; and access control. In cases where significant IT tasks were outsourced, the computer and security knowledge of the contractor were also assessed.

Daily practices assessment

The third objective was to measure the actual use or daily practices of the existing infrastructures and knowledge. The researchers assessed the local governments' enforcement efforts including access control to information systems, such as password policies, and accountability practices, such as monitoring employee activities.

First of a kind research related to local government assessment

Since this research is the first of its kind, there were no benchmarks (or absolute numbers) that could be used to compare the results against. However, the researchers did compare the results between rural and urban municipalities to analyze their similarities and differences.

While the National Institute of Standards and Technology (NIST) offers assessment frameworks and tools to measure security readiness, their main focus is on federal agencies. Currently, there is no government standard that specifically addresses the security readiness of local governments.

Therefore, this project can serve as a solid baseline for follow-up studies.

METHODOLOGY

For the study, the researchers defined local governments as counties, cities, boroughs, townships, and authorities (Martin, 1997). Of these 2,576 municipalities, 1,655 are regarded as rural based on the Center for Rural Pennsylvania's definition as follows (The Center for Rural Pennsylvania, 2007): a municipality is rural when the population density within the municipality is less than 274 persons per square mile or the municipality's total population is less than 2,500 unless more than 50 percent of the population lives in an urbanized area, as defined by the U.S. Census Bureau. All other municipalities are considered urban.

The research project focused primarily on rural municipalities but collected data from urban municipalities for comparison purposes¹.

To promote a balanced representation of all rural counties, the researchers made considerable attempts to survey at least 10 municipalities in each of the state's 46 rural counties with 10 or more municipalities. The surveys were sent to all municipalities in the rural counties of Cameron and Forest, as Cameron has seven municipalities and Forest has nine municipalities.

The researchers developed four surveys: one each for managers, clerical staff, in-house, and outside IT technicians.

The researchers invited all 2,576 local governments in Pennsylvania (out of which 1,655 are rural) to participate in the survey. Respondents from 276 municipalities, including counties, boroughs, cities and townships, participated in the study: 67 percent (184)

were rural municipalities and 33 percent (92) were urban municipalities (See Map 1). A total of 379 individuals responded. Although this response rate was lower than expected, there was adequate representation of the population in the sample at the 95 percent confidence level.

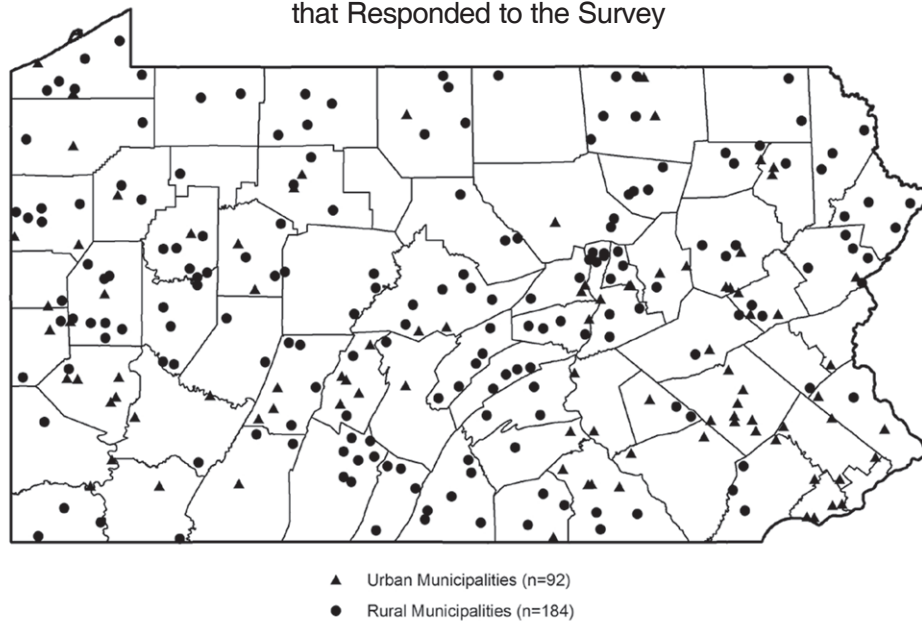
Survey limitations

One limitation of the study is the relatively small sample size of 379 respondents from both urban and rural municipalities. Originally, the researchers aimed to obtain participation from a total of 476 municipalities, from each of which a manager, a clerical person, and possibly an in-house IT technician would participate. However, only 191 managers, 161 clerical staff, and 27 in-house IT technicians participated. Because one of the goals of this study was to compare the rural and urban municipalities rather than managers, clerical staff and IT technicians, the data analysis was performed with all of the data combined from the 379 respondents.

One of the reasons for the lower-than-expected response rate may be the length of the survey. The survey contained a total of 59 questions with some of them having multiple statements and many questions requiring open-ended answers. Another reason for the lower response rate may be that the respondents were concerned about the confidentiality of their information and how the information would be used, once obtained. This may be the case although the cover letter sent to the municipalities and informed consent form contained the statements of confidentiality.

¹ Computers used for police business were not included in the study.

Map 1: Location of Rural and Urban Municipalities that Responded to the Survey



RESULTS

Sample description

The average population of the rural municipalities that responded to the survey was 2,463 in 2008; the average for the urban municipalities that responded was 7,580.

A total of 249 rural (66 percent) and 130 urban municipal employees (34 percent) took the survey. Out of the 379 people who responded to the survey, 65 percent were full-time and 35 percent were part-time employees. Table 1 provides more details about the sample population.

Table 1: Characteristics of Respondents and Their Municipalities

	n	Manager	n	Clerk	n	IT Support	n	Total
Rural	114	60%	124	77%	11	41%	249	66%
Urban	77	40%	37	23%	16	59%	130	34%
Full-time	129	73%	85	54%	20	77%	234	65%
Part-time	48	27%	72	46%	6	23%	126	35%
Average years of employment	175	10.9	147	11	27	8	349	11
Male	108	58%	10	6%	14	54%	132	36%
Female	79	42%	149	94%	12	46%	240	64%
Average Age	147	51	115	51	16	47	278	51
Education	187		159		26		372	
High school	56	30%	85	54%	6	23%	147	40%
2-year college	37	20%	41	26%	12	46%	90	24%
4-year college	43	23%	16	10%	6	23%	65	18%
Master's	35	19%	2	1%	1	4%	38	10%
Doctoral	3	2%	0	0%	0	0%	3	.8%
Other	13	7%	15	9%	1	4%	29	8%

Infrastructure assessment

Infrastructure readiness was assessed using the following criteria: human resources, total budget, security-relevant budget, general hardware infrastructure, security-relevant hardware infrastructure, general software infrastructure, and security-relevant software infrastructure. The definition of each infrastructure readiness measurement is provided in Table 2.

Human resources

In-house IT personnel

Among the rural municipal respondents, about 81 percent indicated they had no in-house IT personnel while about 19 percent had one or more in-house IT personnel. Among the urban municipal respondents, 76 percent said they had no in-house IT person-

Table 2: Infrastructure Readiness Measurements Definitions

Readiness Category	Definition
Human Resources	Measured the number of in-house IT personnel and the percentage of computer hardware and software support outsourced to a third-party contractor.
Total Budget	Measured by the estimated average total dollar amount budgeted during the past five fiscal years.
Security-Relevant Budget	Measured by the estimated average total dollar amount spent on the information systems security hardware and software during the past five fiscal years.
General Hardware Infrastructure	Measured by the number of each computing device type owned by a municipality and used by its employees.
Security-Relevant Hardware Infrastructure	Measured by the number of each computing device type with Internet access.
General Software Infrastructure	Measured by the types of Operating Systems running on a municipality's computers.
Security-Relevant Software Infrastructure	Measured by the types and number of security software installed on a municipality's computers.

nel while 24 percent had one or more in-house IT personnel. There were no statistically significant differences in the number of in-house IT personnel between rural and urban municipalities. Therefore, the researchers concluded that a majority of both rural (81 percent) and urban municipalities (76 percent), in general, lack dedicated IT personnel.

Third-party contractors

About 54 percent of rural respondents and 14 percent of urban respondents did not outsource their computer hardware and software support. Approximately 52 percent of urban municipalities outsourced more than 75 percent of their computer hardware and software support compared to 28 percent of rural municipalities. The differences between rural and urban municipalities were significant. Since most of the rural municipal respondents did not have dedicated IT personnel, this significantly low outsourcing rate for rural municipalities implies they rely heavily on non-IT personnel for their hardware and software support. Table 3 shows a summary of the survey results on the use of third-party contractors.

When comparing the percentages of respondents who did and did not outsource for IT support with those who did or did not have in-house IT support, the researchers found no statistically significant differences. Out of the 80 respondents in both rural and urban municipalities who did not have in-house IT personnel, 65 percent outsourced their IT support and 35 percent did not.

More information on the details of outsourced hardware and software support follows.

- Among rural municipal respondents, 41 percent used in-house network administrators and 39 percent outsourced their network administration. Among urban respondents, 45 percent used in-house network administrators and 37 percent outsourced.
- A majority of rural and urban municipal respondents (88 percent rural and 88 percent urban) performed the data backup function in-house. However, significant differences in the percentage of the in-house and outsourced Web site development and maintenance functions were observed within rural and urban municipalities. Almost 44 percent of the rural municipalities used in-house administration and 30 percent outsourced administration of their Web site development. About 52 percent of urban municipalities used in-house administration and 30 percent outsourced their Web site development.
- Urban municipalities used significantly more in-house resources (59 percent) than rural municipalities (46 percent) to maintain their Web site. Similarly, rural municipalities outsourced more (31

percent) than their urban counterparts (26 percent) to maintain their Web sites. The differences were significant.

- A majority of rural (64 percent) and urban (77 percent) municipalities with Web sites outsourced their Web site hosting.
- A majority of rural (64 percent) and urban (77 percent) municipalities outsourced their software development.
- A majority of rural (66 percent) municipalities used in-house resources to install software whereas urban municipalities used almost an equal percentage of in-house (40 percent) and outsourced (43 percent) software installation.
- A majority of rural (55 percent) municipalities used in-house and a majority of urban (54 percent) municipalities outsourced their software maintenance. The differences were statistically significant.

Table 3: Use of Third-Party Contractors

Use of Third-Party Contractors %	Municipality Type %	
	Rural	Urban
0	54	14
1 - 25	14	11
26 - 75	4	23
76 - 100	28	52
Total	100	100

Total budget

The research found significant differences between rural and urban municipalities in their estimated average total budgets in the past 5 years. Approximately, 49 percent of rural municipalities had budgets ranging between \$100,001 and \$1 million whereas approximately 57 percent of urban municipalities had budgets ranging between \$1,000,001 and \$100 million. Table 4 shows a summary of the survey results on total budgets.

Table 4: Total Budgets

Total Budget Categories	Municipality Type %	
	Rural	Urban
\$0	4	0
\$1 - \$10,000	11	15
\$10,001 - \$100,000	7	7
\$100,001 - \$500,000	31	7
\$500,001 - \$1,000,000	18	14
\$1,000,001 - \$10,000,000	28	47
\$10,000,001 - \$100,000,000	1	10
Total	100	100

Security-relevant budget

The study found significant differences between rural and urban municipalities in the average total dollar amount spent on security hardware and software during the past 5 years. Approximately 25 percent of rural municipalities and 7 percent of urban municipalities spent nothing on information systems security hardware and software during the past 5 years. Almost 64 percent of rural municipalities spent between \$1 and \$10,000 compared to 68 percent of urban municipalities. This was an encouraging sign, showing that both rural and urban municipalities were making investments toward information systems security. Approximately, 21 percent of urban municipalities spent between \$10,001 and \$100,000 on information systems security compared to 11 percent of rural municipalities. No rural municipality spent over \$100,000 and no urban municipality spent over \$150,000 on information systems security.

General hardware infrastructure

Computing devices

In rural municipalities, the average number of desktop computers reported by 143 respondents was about three, the average number of laptop computers reported by 82 respondents was slightly less than one, and the average number of handheld devices reported by 52 respondents was less than one. In urban municipalities, the average number of desktop computers reported by 93 respondents was about 16, the average number of laptop computers reported by 83 respondents was about five, and the average number of handheld devices reported by 64 respondents was about one. The differences between rural and urban municipalities were significant.

Security-relevant hardware infrastructure

Computing devices with Internet access

In rural municipalities, the average number of desktop computers with Internet access reported by 141 respondents was about three, the average number of laptop computers with Internet access reported by 59 respondents was about one, and the average number of handheld devices with Internet access reported by 31 respondents was less than one. In urban municipalities, the average number of desktop computers reported by 93 respondents was about 15, the average number of laptop computers reported by 74 respondents was about five, and the average number of handheld devices reported by 52 respondents was less than one. The differences among rural and urban municipalities were significant. From these findings, the researchers conclude that a good portion of the

municipal-owned desktop computers and laptops were connected to the Internet, which could mean a higher possibility of attacks via the Internet.

General software infrastructure

Operating systems

The survey results showed that Windows XP was the dominant Operating System among all municipalities: 61 percent for rural and 40 percent for urban municipalities. The widespread use of Windows XP was encouraging since the Operating System was mature and supported by Microsoft in terms of security fixes. The support will end, however, in 2014.

Security-relevant software infrastructure

The survey results showed that anti-virus software was the most widely used security software: 86 percent of both rural and urban municipalities had the anti-virus software installed on all of their computers. However, there were five rural municipalities and two urban municipalities that had no anti-virus software installed on any of their computers.

Both rural and urban municipalities also had other well-known types of security software such as firewalls (68 percent) and pop-up blockers (73 percent). About 40 percent of all municipalities had adware remover installed, 40 percent had intrusion detection software and 52 percent had spam filters installed on all their computers. As expected, the adoption rate was fairly low for more advanced types of security software including e-mail monitoring software (9 percent), Virtual Private Network (VPN: allows a secure remote connection between two hosts) (9 percent), and the Internet content filtering software (19 percent).

Computer literacy assessment

Computer literacy readiness was assessed by measuring the following criteria: computer training, computer knowledge, self-assessment of computer knowledge, security training, security knowledge, and self-assessment of security knowledge.

Computer training

Respondents were asked to list all the information-systems-related training, certification, and degrees they had obtained in a class or a self-paced course within the past 5 years. Of the 141 respondents who answered the question, 43 percent said they received no training. About 4 percent had an associate's degree or higher in computer information systems, 33 percent took some courses to learn how to use various software programs including accounting/payroll software such as QuickBooks, Peachtree, the Microsoft Office suite

(consisting of Excel, Word, and Access), Web design software, Adobe, and Exchange 2000. Another 4 percent attended job-related seminars, and 7 percent received a certificate or training in computer software, such as GIS, computer forensics, emergency management, and Web site design/maintenance. About 2 percent were self-taught, and 7 percent received job-related training. In general, it appears that the level of computer training among municipal employees was low.

To collect more detailed information on computer training, the researchers asked respondents how many hours of computer training they completed during the past 12 months in each of the following categories: Microsoft Office applications, accounting software, network software, programming, and Web design.

A majority of the employees in both rural (84 to 99 percent) and urban (74 to 99 percent) municipalities did not receive any training in these areas in the last 12 months. Other training received included wireless security (40 hours), GIS (10 to 16 hours), property records system (8 hours), Caselle (8 hours), payroll (4 to 6 hours), Operating Systems (3 hours), utility billing software (2 to 32 hours), U.S. Census Bureau software (16 hours), Permit-n-Force (8 hours), and state reports (4 hours).

Computer knowledge

A majority of respondents in both rural and urban municipalities knew, on average, the terms: Operating Systems, client, server, portal, router, CPU, main memory, hard drive, Ethernet, Wi-Fi, and bandwidth. Employees in urban municipalities understood all of these terms significantly more than their rural counterparts.

The researchers concluded that both rural and urban municipal officials were knowledgeable about basic computer and networking terms although urban respondents knew significantly more about these terms.

Self-assessment of computer knowledge

Of the 365 respondents who rated their own computer knowledge, 1 percent said they had no knowledge, 22 percent indicated very low to low knowledge, 58 percent indicated average knowledge, and 19 percent indicated high to very high knowledge. The reported knowledge of urban respondents was significantly higher than their rural counterparts.

Security literacy assessment

Security training

For this assessment, respondents were asked about the number of information systems security training

hours they completed during the past 12 months. This training would have covered password use policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper Internet use, and transporting computers or data from authorized locations.

A majority of both rural (more than 92 percent) and urban (more than 89 percent) respondents did not receive any training on password use policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper Internet use, and transporting computers or data from authorized locations in the past 12 months.

Security knowledge

Respondents were asked about their level of knowledge of terms such as Phishing, malware, spyware, botnet, rootkit, computer virus, SQL injection, Denial of Service (DoS), computer worm, wardriving, spam, identity theft, encryption, Virtual Private Network (VPN), anti-virus software, spam filter, adware, intrusion detection system, system log, and firewalls.

Significantly more urban respondents knew the terms Phishing, malware, spyware, computer virus, SQL Injection, DoS, wardriving, spam, identity theft, encryption, VPN, spam filter, adware, system log, and firewalls. Knowledge of the terms botnet, rootkit, computer worm, anti-virus Software, and intrusion detection system was not significantly different between rural and urban respondents. A majority of respondents in both rural and urban municipalities indicated that their knowledge on these terms was below average. A majority of rural respondents stated their knowledge on Phishing, SQL injection, DoS, wardriving, VPN, and system log was below average. This lack of knowledge among rural respondents was concerning since these security threats are so pervasive.

Self assessment of security knowledge

Respondents were asked to describe their information systems security knowledge on a six-point scale ranging from none to very high. Urban respondents' (self-assessed) knowledge of information systems security was significantly higher than that of rural respondents.

Overall, all respondents seemed to be more confident in their computer knowledge than their security knowledge. About 26 percent of rural and 18 percent of urban respondents said their computer knowledge was below average whereas 49 percent of rural and 29 percent of urban respondents said their information systems security knowledge was below average. Out of 363 respondents, 3 percent indicated no knowledge of

Table 5: Use of Third-Party Service Agreements

Third-Party Service Agreement Requirements	Municipality Type %	
	Urban	Rural
Yes	75	32
No	3	7
Do not have service agreement	16	60
Do not know	6	1
Total	100	100

information systems security, 39 percent indicated very low to low knowledge, 48 percent indicated average knowledge, and 10 percent indicated high to very high knowledge.

Daily practices assessment

Daily practices were assessed by measuring the following criteria: service agreement policies, computer sharing, remote access, inventory management, Operating System patch updates, definition file updates, use of encryption methods, information systems security training provided, e-mail handling, data backups, data disposal, physical security, disaster recovery, general security policies, access control, and accountability practices.

Service agreement policies

Respondents were asked whether their service agreement required information systems security precautions, such as regular data back-ups, automated updates of Operating Systems and virus definition files, and if they outsourced to a third-party contractor for computer hardware and software support.

Among urban respondents who contracted with a third-party contractor, 75 percent had service agreements that required information systems security precautions. Among rural respondents with a third-party contractor, 32 percent had service agreements that required information systems security precautions. Sixty percent of rural respondents did not have a service agreement with a third-party contractor compared to 16 percent of urban respondents. This was disconcerting (especially for rural respondents) because service agreements with security precautions are generally recommended for better security. The differences between rural and urban respondents were significant. (See Table 5)

A majority of both rural (75 percent) and urban respondents (80 percent) did not share computers with

other employees in their municipality. About 25 percent of rural and 20 percent of urban respondents shared their computers with others. This was encouraging since avoiding computer sharing is more desirable for information systems security although sharing itself does not necessarily mean bad security. The respondents were also asked how they logged onto their work computers. Most respondents used both a user ID and a password to log on to their computers (57 percent urban and 35 percent rural). Eleven percent of rural respondents and 4 percent of urban respondents did not use a user ID, a password, or other means to log on to their computers. For 25 respondents who provided reasons for other log-in methods, the responses included no log-on required, fingerprint reader on a new laptop, do not use the computer, use a personal computer for work, e-token, and homepage. About 63 percent of rural and 46 percent of urban respondents adopted insecure user name/password practices (i.e., not using anything at all or using only a user ID or password).

The researchers concluded that computer sharing in rural (24 percent) and urban (21 percent) municipalities was done in an insecure manner without the proper use of a user ID and a password.

Amount of Internet use

Rural respondents spent an average of 1.5 hours per day and urban respondents spent an average of 1.9 hours per day on the Internet while at work. The difference was not significant. This implied that both rural and urban municipal employees used the Internet almost equally every day.

Remote access

Significantly more urban respondents than rural respondents remotely connected to their municipalities' computers from home, a café, or other off-site location. A majority of both rural and urban respondents (92 percent rural and 72 percent urban) did not remotely connect to their municipalities' computers.

Inventory management

A majority of both rural and urban respondents said their municipalities kept an inventory of their desktop computers (74 percent rural and 83 percent urban). However, significantly more urban municipalities kept an inventory of their laptop computers (75 percent urban vs. 43 percent rural), handheld devices (53 percent urban vs. 22 percent rural), and other devices, such as faxes and printers (40 percent urban vs. 0 percent rural).

Operating system patch updates

In both rural and urban municipalities, most Operating System patches, which are software upgrades that fix a specific problem with the Operating System, were installed automatically (48 percent rural and 43 percent urban). However, some were installed manually (18 percent rural vs. 15 percent urban), and others were installed both manually and automatically (7 percent rural and 20 percent urban).

Definition file updates

The research found significant differences between rural and urban respondents in their practices of updating definition files, which are lists of known malicious software used by security software when it scans a computer system. In both rural and urban municipalities, definition files were updated mostly automatically (62 percent rural and 53 percent urban). However, a higher percent of urban municipalities updated their definition files both manually and automatically (18.5 percent urban and 3.5 percent rural).

Use of encryption methods

No significant differences were found between rural and urban respondents in terms of encryption methods used. A majority of all respondents did not know what encryption method was used in their municipalities (63 percent rural and 57 percent urban). This was concerning since encryption is critical in protecting data sent wirelessly.

Information system security training provided

A majority of both rural and urban respondents provided no training on password use policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper Internet use, and transporting computer and data from authorized locations. However, the percentage was significantly higher among rural respondents than urban respondents.

The percent of training on password use policies (16 percent rural and 24 percent urban), data access and authorization policies (14 percent rural and 25 percent urban), computer security attack precautions (8 percent rural and 17 percent urban), proper disposal of sensitive data (11 percent rural and 18 percent urban), policies for proper Internet use (14 percent rural and 30 percent urban), and transporting computer and data from authorized locations (9 percent rural and 16 percent urban) provided in urban municipalities for new hires was significantly higher than that of rural.

Table 6: Summary of E-mail Handling

Actions Taken When Reading Email	Municipality Type %	
	Urban	Rural
1. Don't open email from a stranger	3	2
2. Don't open attachments from a stranger	2	2
3. Don't click on any hyper-links in a suspicious email	4	3
All of the above	71	76
Any combination of 1, 2 & 3	20	13
Do not take any action	0	4
Total	100	100

E-mail handling

A majority of both rural and urban respondents said they did not open e-mails and attachments from a stranger (76 percent rural and 71 percent urban) and did not click on any hyperlinks in a suspicious email (9 percent rural and 16 percent urban). Other actions reported by the respondents included the use of a spam/sender blocker, disable image preview, anti-virus software, downloaded an AVG free version, and preferences set to the highest level. This finding was encouraging since a majority of respondents seemed to take proper actions when receiving suspicious e-mails. However, even the small number of respondents who did not take proper actions could create vulnerabilities for municipal information systems security. (See Table 6)

Data back-ups

Significant differences in the data back-up practices were found between rural and urban respondents, as a higher percentage of urban respondents backed up their data daily (42 percent rural and 73 percent urban). A higher percentage of rural municipalities backed up their data monthly (17 percent rural and 3 percent urban). The researchers concluded that both rural and urban respondents backed up their data regularly although there were differences in frequencies.

Almost 29 percent of rural respondents never tested their backup data to see if it worked compared to almost 19 percent of urban respondents. Approximately 23 percent of rural respondents said they check their backup data monthly compared to 17 percent of urban respondents and 19 percent of rural respondents and 25 percent of urban respondents said they did not know the answer to this question. Lastly, the respondents were asked where their municipality stored backup files. A majority of both rural and urban

respondents said their municipalities kept their backup files mostly onsite (reported as in a safe, server hard drive, flash drive, CDRW & multiple hard drives, fire-proof filing cabinet, locked cabinet, shelf, drawer, municipal building, on each other's PC, and always with themselves). Approximately 31 percent of both rural and urban respondents kept their backup files at an offsite location (reported as employees' home, safe deposit box, another building, and online backup). This finding was alarming because storing backup files on site is not a recommended security practice.

Data disposal

Respondents were asked what methods their municipalities used to dispose of paper documents that contained sensitive and confidential information. A majority of both rural (80 percent) and urban (91 percent) respondents said their municipalities used shredders. However, a higher percentage of rural (10 percent) respondents cited burning as a means of disposal than urban (1 percent) respondents.

Respondents were also asked how their municipalities disposed of devices containing sensitive and confidential information, such as old computers, external hard drives, USB drives, and CD/DVD.

Many respondents did not know the disposal methods for electronic media with data. Among those who did know, a high percentage said they first erased the data and then either trashed or recycled the device. Others erased the data and then destroyed the device. Some never had to dispose of electronics and a small percentage said disposal was handled by a third-party professional company/person.

From these responses, the researchers concluded that municipalities adopted good practices when disposing of paper documents, but not when disposing of electronics and their media.

Physical security

A majority of both rural and urban respondents did not use locks on their computers, surveillance cameras, burglar alarms, key card systems, or key pad systems for entry. However, a majority of both respondents used door locks and had backup power supplies. The percent of urban respondents using backup power supplies (85 percent) was higher than rural (58 percent).

Approximately 25 percent of rural and 29 percent of urban respondents used other types of physical security tools, including password-protected computers, biometric access systems, and cameras. A majority of rural respondents (64 percent rural and 29 percent urban) did not use other physical security tools, and a

majority of the urban respondents (11 percent rural and 43 percent urban) did not know of other security-related tools that were being used.

These results indicated that a majority of municipalities were equipped with a bare minimum set of physical security tools and that there is much room for improvement in introducing more advanced physical security equipment.

Disaster recovery

Respondents were asked whether they had an alternate site to keep their municipality operational if their office building was damaged or became unusable due to fire, flood, or other reasons. A majority of both rural (57 percent) and urban (67 percent) respondents said their municipalities had an alternate site.

General security policies

A majority of both rural and urban respondents said their municipalities did not have policies in written form on the proper disposal of sensitive data (84 percent rural and 66 percent urban), disaster recovery (82 percent rural and 68 percent urban), and data backup (82 percent rural and 68 percent urban).

Access Control

Take home equipment

A majority of both rural (78 percent for laptops and 54 percent for storage devices) and urban (53 percent for laptops and 48 percent for storage devices) respondents were not permitted to take equipment off-site. However, a significantly higher percentage of urban respondents (45 percent) were permitted to take laptops off-site than rural respondents (17 percent).

A majority of both rural (72 percent for laptops and 63 percent for storage devices) and urban (50 percent for laptops and 52 percent for storage devices) respondents did not connect their laptops and data storage devices to their home network. However, a significantly higher percentage of urban respondents (38 percent) connected their laptops (37 percent) and data storage devices (37 percent) to their home network than rural (18 percent laptops and 31 percent data storage devices).

Password management

A majority of the rural (64 percent) and urban (57 percent) respondents said they were never required to change passwords. There was no daily or weekly requirement for changing passwords. A smaller percentage of both rural and urban respondents were required to change passwords either monthly or quarterly. Some of the open-ended answers to this

question included: passwords are changed when a new employee is hired, passwords are changed when an employee feels it's necessary, the computer is set up to change passwords every 90 days, and I am the only one using the township computer. Responses to this question were alarming since periodically changing passwords is a recommended security practice.

Management of sensitive resident information

Respondents indicated they did not store any credit card numbers of residents. Typically, municipalities store names and addresses of residents, followed by phone numbers, other types of information, tax ID numbers, and Social Security Numbers (SSN: 4 percent rural and 2 percent urban). Other types of information included utility billing information, property ID numbers, tax parcel/permit numbers, and home assessed values. This finding was encouraging because the information stored on municipal computers was minimal.

Policies

A majority of rural (91 percent) and urban (81 percent) respondents said their municipalities did not have a password expiration policy. However, a significantly higher percentage of urban respondents said their municipality had a strong password use (5 percent rural and 15 percent urban) and password expiration (4 percent rural and 8 percent urban), and data access and authorization (8 percent rural and 21 percent urban) policies than rural municipalities. Almost equal percentages of both rural (89 percent) and urban (81 percent) respondents said their municipalities did not have a policy on transporting computers/data storage devices from authorized locations.

Accountability Practices

Network monitoring

A majority of both rural (63 percent) and urban (51 percent) respondents said their municipalities did not monitor the logs of network connection activities. This was unexpected since network monitoring is a recommended security practice.

Personal use of computers

Approximately one-half of both rural (51 percent) and urban (50 percent) respondents said they were aware or very aware of how the employees in their municipality were using computer systems for their personal uses.

Policies

A majority of rural (82 percent) and urban (48 percent) respondents said there were no written policies on Internet use.

Respondents were also asked about the number of information systems security-related incidents that occurred due to a computer security attack that may have resulted in the loss of sensitive and confidential data, data corruption, computer system malfunction, and other incidents. Regarding the loss of sensitive and confidential data, only one incident was reported from the 119 rural respondents who answered the question. The incident involved a virus that was downloaded from an email; however, files were recovered from a backup device. Among the 86 urban respondents who answered this question, no incidents were listed.

Few incidents due to data corruption, computer system malfunction, and other issues were reported.

Perceived readiness

Respondents were asked how they would rate (1) the overall preparedness of their municipality for preventing hacking attempts from the Internet, which could compromise information systems at work, (2) the overall physical security of their office building for preventing the theft of their computers, data storage devices, and/or paper documents that contain sensitive information, and (3) the overall preparedness of their office building for its ability to recover and become operational after a disaster, such as fire, floods, and terrorist attacks.

Significant differences were found between rural and urban respondents in their perceptions of preparedness for preventing hacking attempts and the theft of their computers, data storage devices and/or paper documents, and their ability to recover and become operational after a disaster. Among urban respondents, 67 percent said their municipality was somewhat to very prepared compared to 54 percent of rural respondents. Almost 75 percent of urban respondents said their municipal buildings were somewhat to very prepared for preventing theft compared to approximately 71 percent of rural respondents. Almost 70 percent of urban respondents said their municipal building was somewhat to very prepared to recover and become operational after a disaster compared to almost 61 percent of rural respondents.

CONCLUSIONS

In terms of infrastructure readiness, the researchers identified the following factors that may challenge the security readiness of rural municipalities

- Human resources: both rural and urban municipalities, in general, lacked dedicated IT personnel. Most urban respondents outsourced their computer hardware and software support, which was significantly more than rural respondents. Considering that most rural respondents did not have dedicated IT personnel, the researchers concluded that many rural municipalities relied heavily on non-IT experts for computer hardware and software support. The survey results indicated that approximately half of the rural municipalities had neither in-house nor outsourced computer hardware/software support. Regarding the question of what was done in-house and what was outsourced, the responses from both rural and urban respondents were very similar, especially in terms of network administration (both done in-house), Web site hosting (both outsourced), and software development (both outsourced). They differed, however, in other functions, such as Web site development and maintenance (rural outsource, urban in-house), and software installation and maintenance (rural in-house, urban outsource).
- Security-relevant budget: overall, rural respondents said their municipalities spent much less money on information systems security. Approximately 25 percent of rural respondents spent nothing on information systems security compared to 7 percent of urban respondents who spent nothing in the past 5 years.
- Security-relevant hardware infrastructure: most of the municipality-owned desktop computers and laptops were connected to the Internet, which increased the possibility of attacks via the Internet. Both rural and urban municipalities commonly used the Internet for e-mail, searches, and online purchases. Both rural and urban municipal employees used the Internet every day.
- Security-relevant software infrastructure: as expected, the adoption rate was low for more advanced types of security software including spam filters, intrusion detection systems, adware removers, Internet content filtering software, Virtual Private Networks (VPN), and e-mail monitoring software. Some security software, such as anti-virus software, pop-up blockers, firewalls, and adware removers, is more effective when it is installed on all the computers in a network. It was concerning that many

respondents, especially rural respondents, indicated that their municipalities had a number of unprotected computers.

The researchers identified the following areas as relative infrastructure readiness strengths of rural municipalities:

- Software infrastructure: 61 percent of rural and 40 percent of urban respondents said their municipalities used Windows XP. The widespread use of Windows XP was encouraging since the Operating System is mature and still supported by Microsoft through various security fixes.
- Security-relevant software infrastructure: the survey results showed that anti-virus software was the most widely used security software. Around 83 percent of rural and 90 percent of urban respondents said their municipalities had the anti-virus software installed on all of their computers. This trend continued with other well known types of security software, such as firewalls and pop-up blockers. The most common anti-virus software used was Norton and McAfee.

In terms of literacy readiness, the researchers identified the following factors as potential weaknesses of rural municipalities.

- Computer training: in general, the level of computer training among municipal employees was low. A majority of rural respondents (84 to 99 percent) and urban respondents (74 to 99 percent) had not received any computer training (on Microsoft Office applications, accounting software, network software, programming, and Web design) for 12 months prior to the survey.
- Security training: a majority of respondents from both rural and urban municipalities had not received any training on password use policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper Internet use, and transporting computers or data from authorized locations for the 12 months prior to the survey.
- Security knowledge: a majority of respondents from both rural and urban municipalities indicated their knowledge on basic security terms, particularly, Phishing, SQL injection, DoS, wardriving, VPN, and system log, was below average. However, urban respondents knew significantly more about these terms.
- Self-assessment of security knowledge: unlike the more confident answers to the self-assessment of

computer knowledge question, 71 percent of urban and 51 percent of rural respondents stated that their information systems security knowledge was above average.

The following two areas were identified as relative literacy readiness strengths of rural municipalities.

- Computer knowledge: both rural and urban respondents were knowledgeable about basic computer and networking terms, although urban respondents knew significantly more about the same terms.
- Self-assessment of computer knowledge: a majority of rural respondents (73 percent) said their computer knowledge was average or above average. However, urban respondents' self-assessment of their computer knowledge was significantly higher.

For daily practices readiness, the researchers identified the following areas as potential weaknesses of rural municipalities.

- Service agreement policies: only 32 percent of the contracts between rural municipalities and a third-party contractor required information systems security precautions, such as regular data backups, automated updates of Operating Systems, and anti-virus definition files. Almost 60 percent of rural respondents indicated their municipalities did not have a service agreement with a third-party at all. This was alarming since creating a service agreement and ensuring that security precautions are part of the document are recommended for better security.
- Access control: a majority of rural respondents (63 percent) adopted insecure user name/password practices, such as not using anything at all or using only one of them. Although relatively rare, computer sharing in rural municipalities (24 percent) was conducted in an insecure manner without the proper use of a user ID and a password. In addition, a majority of rural respondents (64 percent) indicated they were never required to change passwords.
- Use of encryption methods: A majority of rural respondents did not know what encryption method was used in their wireless local area networks.
- Information systems security training provided: a majority of rural respondents said their municipalities did not provide information systems security training on password use policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper Internet use, and transporting computer and data from authorized locations.
- Data backup: a majority of rural respondents said their municipalities backed up their data but did not verify the backup as often as necessary.
- Physical security: a majority of rural respondents

said their municipalities were equipped with a bare minimum set of physical security tools, such as door locks and backup power supplies. There was much room for improvement in introducing more advanced physical security equipment to these municipalities, however.

- Data disposal: a majority of rural respondents said their municipalities adopted good practices when disposing of paper documents but not when disposing of computers and their media.
- General security policies: a majority of rural respondents said their municipalities did not have policies in written form on the proper disposal of sensitive data, Internet use, disaster recovery, data backup, strong password use policy, password expiration policy, data access and authorization policy, and transporting computers/data storage devices from authorized locations.
- Accountability practices: a majority of rural respondents said their municipalities did not monitor the logs of network connection activities. It also appeared that more work needed to be done to improve management's awareness of employees' use of their computers for personal purposes.

The following areas were identified as relative daily practice strengths of rural municipalities:

- Computer sharing: a majority of respondents did not share computers.
- Remote access: a majority of respondents did not remotely connect to their municipalities' computers.
- Inventory management: a majority of respondents kept an inventory of their desktop computers although laptops and hand-held devices were not managed as well as the desktops in rural municipalities.
- Operating System patch updates: Operating System patches were installed mostly automatically.
- Definition files updates: definition files were updated mostly automatically.
- E-mail handling: a majority of respondents took proper actions when receiving suspicious e-mails.
- Data backup: a majority of respondents said their municipalities backed up their computer data regularly.
- Disaster recovery: a majority of respondents said their municipalities had an alternate site to keep their municipality operational if their office building was damaged or became unusable. However, almost one-third indicated they did not have an alternate site.
- Access control: a majority of respondents were not permitted to take laptops off-site. A majority also did not connect their laptops and data storage devices to their home network. These findings were encourag-

ing for rural municipalities since having less take-home equipment connected to one's home network is better for security.

- Management of sensitive residential information: the respondents indicated they did not store credit card numbers. Names and addresses of residents were the most commonly stored information, followed by

phone numbers, other types of information, tax ID numbers, and Social Security Numbers.

From these findings, the researchers concluded that, while there were positive signs of security readiness, there were many aspects of information systems security that required the attention of rural municipalities.

POLICY CONSIDERATIONS

Pennsylvania state government recognizes the importance of computer information systems security. Led by the Chief Information Officer (CIO) of the state, the Pennsylvania Information Sharing and Analysis Center (PA-ISAC) embodies this awareness and promotes enhancing the state's "cyber security readiness and response" (Commonwealth of Pennsylvania, 2007). In regard to local governments, the primary focus of PA-ISAC has been on raising awareness and providing educational materials rather than developing and imposing policies.

Conversations with officials from rural Pennsylvania municipalities and representatives of county, borough, and township associations indicated that there were few statewide policies or programs in place that monitored, regulated, or trained local government employees in computer information systems security technologies and best practices.

Local government action

Based on their findings, the researchers recommend the following considerations for rural municipalities:

- Resource pooling: one of the major findings of this research was that rural municipalities lacked in-house IT support, not to mention personnel with information systems security expertise. It may be advantageous for small, rural municipalities to pool human resources in both IT and security since the cost of employing IT and security personnel may be prohibitive to these municipalities.
- Periodic assessments: assessing information systems security readiness should not be a one-time exercise. Assessment efforts need to be continuous to ensure that progress is made toward better security environments.
- Written policies on sound security practices: few rural municipalities had written security policies. Creating security policies is the very first step that needs to be taken before anything can be done to improve security. The researchers strongly recommend that municipalities adopt documented security policies.

State government action

- Awareness training and security education: this study found that insufficient training was provided to municipal employees for both computer and information systems security topics. The researchers offer that raising awareness and providing education is critical to significantly increase information systems security readiness and to address many undesirable daily practices pointed out in this study.

- Incident management: the researchers found that, currently, there is no central reporting mechanism that keeps track of information systems security incidents occurring in small municipalities. Having a single incident repository would be highly beneficial, since it would allow municipal officials to quickly identify common information systems security threats specific to their municipalities and to respond to these threats more effectively.

- A Web portal specializing in local government information systems security: the researchers recommend the development of a Web 2.0 style online portal to exchange information and ideas on how to tackle daily information systems security challenges facing small, rural municipalities. This portal would be a thematic Web site that has a collection of links leading to other Internet sites concerning computer security in local governments. Web 2.0 means Web pages built to accommodate user-generated contents, such as blogs, Wikis, and YouTube.

Legislative support

As with many other states, Pennsylvania has its own laws on computer offenses, as described in the Pennsylvania Consolidated Statutes on Crimes and Offenses (also called Title 18). More specifically, Sub-chapter B, section 33 of Chapter 39 (Theft and Related Offenses) of the statutes defines unlawful use of computers. Act 226 of 2002 amended Title 18 by adding Chapter 76 (Computer Offenses) that is much more concrete on describing the types of possible computer crimes and penalties. The laws define what

constitutes computer crimes such as disruption of service, computer theft, unlawful duplication, distribution of computer virus, and Internet child pornography.

Also in 2005, the Breach of Personal Information Notification Act (Act 94) imposed a penalty for not notifying residents whose personal information may have been disclosed as the result of a security breach. And in 2006, the Privacy of Social Security Number Act (Act 60), made it illegal to “intentionally communicate or otherwise make available to the general public” any individual’s Social Security Number.

These efforts in the legislature show that state lawmakers are concerned about citizens’ computer security and privacy. However, all these laws are very generic and do not address local-government-specific concerns. Other states have laws particularly geared toward local governments. For example, in Illinois, the Compiled Statute 5/16D-4 (Aggravated Computer Tempering) states that “a person commits aggravated computer tempering when he knowingly causes disruption of or interference with vital services or operations of state or local government.” The findings from this research may well suggest the need for similar legislation in Pennsylvania.

Despite their vagueness, the state laws mentioned above do have a potential to be used to make rural municipalities liable to negligence law suits. After all, each local government is ultimately responsible for the information systems, data, and actions of its employees under its control if proper actions were not taken to minimize the possibility of computer security attacks.

At the federal government level, there are two computer information systems security laws that may affect rural municipalities. One of these laws is the Sarbanes-Oxley Act of 2002, which requires organizations “to establish, monitor, and report on the effectiveness of controls that ensure the integrity and accuracy of financial data.” The other is the Federal Information Security Management Act (FISMA) that mandates information systems security protection among federal agencies and their partners.

Federal funding

The Computer Crime Enforcement Act (Public Law 106-572) was enacted in December 2000. The law establishes “a grant program to assist state and local law enforcement in deterring, investigating, and prosecuting computer crimes.” The findings from this research project may help Pennsylvania win such a federal grant by providing concrete evidence for the necessity of more funding.

References

- Chew, E., A. Clay, J. Hash, N. Bartol, and A. Brown. (2006) "A Guide for Developing Performance Metrics for Information Security." National Institute of Standards and Technology (NIST) Special Publication 800-80. Technical Report, U.S. Department of Commerce, May 2006.
- Commonwealth of Pennsylvania. (2007) PA-ISAC. Accessed at <http://www.cybersecurity.state.pa.us/portal/server.pt?open=512&objID=337&&PageID=195784&mode=2>, July 2007.
- Computer Security Institute. (2008) *2006 CSI Computer Crime and Security Survey*. Accessed at http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.
- Esposito, R. (2006) "Hackers Penetrate Water System Computers." Accessed at http://blogs.abcnews.com/theblotter/2006/10/hackers_penetra.html, July 2006.
- Krouk, D. (2004) "Cyber Security at the Grass Roots." *Planning*, 70, July 2004.
- Martin, J. (1997) *Pennsylvania Almanac*. Stackpole Books, Mechanicsburg, PA, 1997.
- McConn, C.E., J. Ryoo, and T. Girard. (2007) "Assessing the Computer Information Systems Security: Three Case Studies of Local Governments in Central Pennsylvania." *Journal of International Business Research*, 6(1): 55-75, 2007.
- National Association of State Chief Information Officers (NASCIO). (2006) Findings from NASCIO's Strategic Cyber Security Survey, January 2006.
- The Center for Rural Pennsylvania. (2007) *Rural/Urban PA*. Accessed at http://www.ruralpa.org/rural_urban.html, July 2007.
- The Center for Rural Pennsylvania. (2003) *Municipal Computer Use*. Accessed at <http://www.ruralpa.org>.
- Web Application Security Consortium. (2007) *List of Incidents of Class SQL Injection*. Accessed July 2007 at http://www.webappsec.org/projects/whid/list_class_sql_injection.shtml.

**The Center for Rural Pennsylvania
Board of Directors**

*Senator John R. Gordner
Chairman*

*Representative Tina Pickett
Vice Chairman*

*Senator John Wozniak
Treasurer*

*Dr. Nancy Falvo
Clarion University
Secretary*

Representative Tim Seip

*Dr. Theodore R. Alter
Pennsylvania State University*

*Dr. Stephan J. Goetz
Northeast Regional Center
for Rural Development*

*Dr. Keith T. Miller
Lock Haven University*

*Dr. Robert F. Pack
University of Pittsburgh*

*William Sturges
Governor's Representative*



The Center for Rural Pennsylvania
625 Forster St., Room 902
Harrisburg, PA 17120
Phone (717) 787-9555
Fax (717) 772-3587
www.rural.palegislature.us
1P1109-400