Executive Summary

Information Systems Security Readiness Assessment for Municipalities in Pennsylvania

By: Jungwoo Ryoo, Ph.D., Syed Rizvi, Ph.D., and William Aiken, M.S.,
Pennsylvania State University-Altoona
and Brooke Long-Yarrison, Ph.D.

September 2020

There is a broad consensus on the need for a periodic and comprehensive assessment of the information systems security readiness of Pennsylvania municipalities.

This research, modeled after a similar project conducted in 2009, investigated the level of security readiness of Pennsylvania townships and boroughs through an online survey. The survey focused on three major information systems security elements: (1) infrastructure, (2) literacy, and (3) actual use. The infrastructure aspect measured each municipality's access to security-relevant resources, such as security software, physical security countermeasures, human resources, and outsourcing. Literacy addressed whether a municipality had a clear set of security policies, procedures, standards, and guidelines and whether its employees were aware of them beyond their computer knowledge. Actual use examined how properly municipal employees practiced their security knowledge and used their security infrastructure daily.

Outcomes/Results

Managers/administrators and secretaries employed in Pennsylvania's 1,592 rural municipalities and 970 urban municipalities were invited to participate in the survey. In total, 388 municipal employees responded to the survey: 252 (64.9 percent) from rural municipalities and 136 (35.1 percent) from urban municipalities. This provided a response rate of 15.1 percent.

Following are some of the survey results in each of the readiness categories, along with a table comparing the 2009 and 2020 study results.

Infrastructure readiness

The infrastructure readiness category was subdivided into measurements assessing the municipal readiness for (1) internal versus external information technology (IT) services and resources, (2) website security, (3) IT & security budget, (4) current risk environment, (5) business continuity/disaster recovery planning, (6) physical security, (7) logical access control, and (8) inventory. Overall, the research indicated the following:

- Internal vs. external IT services and resources: In general, both rural and urban municipalities lacked dedicated IT personnel. The majority of both rural (84.3 percent) and urban (81.3 percent) respondents said their municipality had zero in-house IT personnel. More urban respondents (70.5 percent) said their municipalities outsourced their computer hardware and software support entirely than rural respondents (55.8 percent). Since most of the rural municipal respondents did not have dedicated in-house IT personnel, the significantly lower outsourc-

The Center for Rural Pennsylvania
A Legislative Agency of the Pennsylvania General Assembly

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, (717) 787-9555, info@rural.palegislature.us, www.rural.palegislature.us.

ing rate for external personnel indicates that rural municipalities may be relying heavily on non-IT experts for their computer hardware and software support.

- Security-relevant budget: Among rural respondents, 99 percent said their municipalities spent $29,999 or less yearly on information systems security software and hardware as compared to 75 percent of urban respondents who said their municipalities spent $29,999 or less. Overall, rural municipalities spent much less money on information systems security.
- Security-relevant hardware infrastructure: Most municipally owned desktop computers and laptops were connected to the internet, which increases the possibility of attacks via the internet. Both rural and urban respondents said they used the internet daily and commonly used it for e-mails, searches, and online purchases.
- Security-relevant software infrastructure: Both rural and urban respondents reported lower adoption rates for more advanced types of security software including spam filters, intrusion detection systems, adware removers, internet content filtering software, Virtual Private Network (VPN), and e-mail monitoring software. Security software is more effective when it is installed on all the computers in a network. It was concerning that both rural and urban municipalities had unprotected computers.
- Physical security: 16.7 percent of urban municipalities use smart cards with RFID (radio frequency identification) to access their building as compared to only 2.3 percent of rural municipalities Additionally, only 57.1 percent of urban municipalities report using mechanical locks as compared to 74.3 percent of rural municipalities.
- Logical access control: A majority of rural (80.8 percent) and urban (99.1 percent) respondents adopted usernames/passwords to control access to their computers. However, it was concerning that 10.8 percent of rural respondents were not using any access control at all. If computer sharing is occurring among municipal employees, it is not secure without the proper use of user IDs and passwords or any other means of access control, such as PIN numbers and fingerprints. Two-factor authentication is a stronger form of access control, but a majority of both rural (91.4 percent) and urban (89.3 percent) respondents have not adopted them.

Literacy readiness

The literacy readiness category was subdivided into measurements assessing the municipal readiness for (1) information technology literacy and (2) information systems security literacy. The research found the following:

- Information systems security knowledge: Both rural (54.3 percent) and urban (51.3 percent) respondents indicated that their knowledge on information systems security was below average. More urban respondents (11.9 percent) rated their current knowledge of information systems security as "high" compared to rural respondents (3.8 percent).

Daily practices readiness

The daily practices readiness category was subdivided into measurements assessing the municipal readiness for (1) application usage and security requirements, (2) software updates, (3) shared environment and security, (4) training, (5) backups, (6) disposal of hardware and sensitive documents, (7) business continuity plans and preparedness, and (8) security policy and procedures. The research found that:

- Security-relevant software infrastructure: While a majority of both rural (89.9 percent) and urban (92.5 percent) respondents had anti-virus software installed on their computers, the adoption rate for more advanced types of security software, including spam filters, intrusion detection systems, adware removers, internet content filtering software, Virtual Private Network (VPN), and e-mail monitoring software was lower. Security software is more effective when it is installed on all the computers in a network. It was concerning that both rural and urban municipalities had unprotected computers.
- Security policy and procedures: Rural (58.8 percent) and urban (45.5 percent) respondents said they never change their passwords. This was alarming since periodically changing passwords is a strongly recommended security practice.
- Use of encryption methods: A majority of both rural (62.1 percent) and urban (66.0 percent) respondents did not know what encryption method was used in their wireless local area networks. This was alarming since encryption is critical in protecting data sent wirelessly.
- Computer training: In general, the majority of rural and urban respondents reported zero hours of training for any computer software and skills, including Microsoft Office, accounting software, network soft-

Comparison of 2009 and 2020 Study Results						
		2009		2020		Analysis
	Factors	Rural	Urban	Rural	Urban	
Infrastructure	Human Resource *(Zero in-house IT personnel)*	81%	76%	84.3%	81.3%	Deteriorated
	IT & security budget *($0 Spending)*	25%	7%	12.1%	1.8%	Substantially improved
	Sec. Relevant Software *(Antivirus - all computers)*	86.1%	86.1%	89.9%	92.5%	Slightly improved
	Disaster recovery planning *(No policy at all)*	82%	67.5%	77.1%	53.1%	Slightly improved
	Logical access control *(No restriction)*	11.3%	4%	10.8%	0%	Slightly improved for Urban
Literacy	Self-Assessment of Computer Knowledge (*average*)	59.4%	71.2%	72.7%	Greater than 72.2%	Improved for Rural
	Self-Assessment of Security Knowledge *(average or above)*	51%	71%	45.6%	48.6%	Substantially Deteriorated
Daily Practice	Service Agreement *(requires ISS precautions)*	32%	75%	62.1%	86%	Improved for Rural & Urban
	Security Software Updated *(automatically)*	61.8%	53.3%	60.9%	50%	Not changed
	Use of Encryption Method (*knowledge)*	63%	57%	62.1%	66%	Deteriorated for Urban
	Accountability practice *(not checking net. logs)*	63.2%	50.5%	75.3%	36.3%	Deteriorated for Rural & Improved for Urban
	Remote Access *(No remote connection)*	92%	72%	88.6%	61.6%	Not changed
	Data Backup	Majority (regularly)	Majority (regularly)	38.7% (daily)	71.8% (daily)	Not changed
	Security training *(0 hr training)*	Majority	Majority	Majority	Majority	Not changed
	Computer Training *(0 hr training)*	Majority	Majority	Majority	Majority	Not changed

ware, programming, web design, and other general computer training.

- Security training: A majority of both rural (87.3 percent) and urban (81.1 percent) respondents had not received any training on password usage policies, data access and authorization policies, computer security attack precautions, proper disposal of sensitive data, policies for proper internet usage, and transporting computers or data from authorized locations for the 12 months prior to the survey.
- Data backups: A majority of both rural and urban respondents said they backed up their data. However, there was a significant difference between rural and urban respondents in terms of how often they backed up files: 71.8 percent of urban respondents backed up files daily, compared to 38.7 percent of rural respondents. And, 5.8 percent of rural respondents said they never backed up their data.
- Data disposal: A majority of both rural (95.3 percent) and urban respondents (97.1 percent) adopted good practices when disposing of paper documents, but some disposed of their computers "as is" (6.4 percent rural and 8.2 percent urban), as well as their media.
- General security policies: A majority of rural respondents said their municipalities did not have written policies on the proper disposal of sensitive data, internet usage, disaster recovery, data backup, strong passwords, password expirations, data access and authorization, data backup, social media, and transporting computers/data storage devices from authorized locations. There was a statistically significant difference between rural and urban responses for general security policies except for those on strong passwords and transporting computers/data storage devices from authorized locations. Urban respondents were more likely to say they had policies.
- Accountability practices: A majority of rural respondents (75.3 percent) said they did not monitor the logs of network connection activities, while 36.3 percent of urban respondents said they did not monitor activity logs.

Policy Considerations

Based on the research findings, the researchers recommend the following policy considerations:

- Resource pooling among different municipalities to share IT staff with security expertise;
- Periodic assessment of information systems security readiness among rural and urban municipalities to monitor progress or any potential deterioration;
- Awareness training and security education among municipal employees;
- A centralized incident management system that keeps track of security breaches and recognizes patterns that surface, if any;
- Written policies for enforcing sound, daily information systems security practices; and
- A website that promotes community-driven exchanges of ideas, and that features a multimedia knowledge base specializing in local government-specific information systems security recommendations.

Visit www.rural.palegislature.us for the full report, *Information Systems Security Readiness Assessment for Municipalities in Pennsylvania*.

The Center for Rural Pennsylvania
www.rural.palegislature.us
1P0920 – 350