Cybersecurity:

Protecting Local Government Digital Resources

ICMA | Microsoft

ICMA, the International City/County Management Association, advances professional local government through leadership, management, innovation, and ethics. ICMA provides member support, publications, data, and information; peer and results-oriented assistance; and training and professional development to more than 10,000 city, town, and country experts and other individuals and organizations throughout the world. The management decisions made by ICMA's members affect 185 million individuals living in thousands of communities, from small villages and towns to large metropolitan areas.

At **Microsoft**, we realize that the customers we serve are the same as those served by governments: our citizens. So, we're committed to helping governments find the right information technology solutions, share resources, and connect across multiple agencies and disparate systems. When governments work together better, it's the public that sees the benefits. Microsoft has created programs designed to help address the unique challenges faced by governments around the world. Partnerships developed through government programs enable Microsoft to help governments become more secure, improve their operations, and begin to close the digital divide more efficiently. Working to address the unique requirements of government organizations, Microsoft has designated enormous resources toward identifying and meeting these needs. More than 1,000 Microsoft employees worldwide work solely on developing technology and programs specifically for the public sector.

Cited Internet sources were valid as of May 2017. Because URLs and websites are constantly changing, we cannot vouch for their current validity.

To locate other ICMA print and digital publications, please visit **icma.org/press**
Cybersecurity: Protecting Local Government Digital Resources

Contents

Foreword iv

Chapter 1. Introduction....................1

Chapter 2. Local Government Cybersecurity in the United States: Survey Reveals Problems and Practices 4

Chapter 3. A Plan for Cybersecurity....................14

Chapter 4. The Cloud and Enterprise Cybersecurity: Leveling the Playing Field....................17

Chapter 5. Cybersecurity Case Studies 21

DeKalb County, Georgia—Community Profile 21

Jefferson County, Alabama—Community Profile 26

City of Roseville, California—Community Profile 29

About the Authors....................33

Appendix A-1: Summary Report of Survey Results....................34

Appendix A-2: Cybersecurity 2016 Survey....................40

Appendix B: Measures of Cyberattacks and Cybersecurity Preparedness 50

Appendix C: Annotated List of Online Cybersecurity Resources 57

Foreword

The speed at which the technology sector has evolved over the past three decades is breathtaking. Most of the advances in technology have been for the good of local governments, moving them from inefficient and costly paper systems for asset management to digital systems that allow local governments to better analyze and understand the full implication of policy decisions.

Such advantages come at a price. Cyber attacks are on the rise, and many local governments now purchase cybersecurity liability insurance to protect them from the potential expenses associated with attack recovery. Replacing data due to loss or theft, requiring unanticipated staff overtime, implementing new software solutions—all cost money if a computer system is shut down due to a malware or ransomware incident.

ICMA (the International City/County Management Association) understands how critical technology is in this digital age for delivering services to community residents. Our members must be aware of what it takes to protect their computer systems and what current and future leading practices may look like. To that end, we are pleased to have worked with our strategic partner Microsoft on the development of this important report on cybersecurity and what policies and procedures local governments are undertaking to protect their computer systems from attacks.

This report is one in a series on technology for local governments and how communities are taking a smart approach to using technology in planning their day-to-day operations. Future reports will look at related topics, such as data analytics, spatial analysis, and mapping, to name a few. The ICMA Smart Communities Advisory Board will also work with ICMA staff to determine what other critical information our members need to stay abreast of current advances in the field.

I hope this volume succeeds in expanding your understanding of the challenges and necessity of cybersecurity. ICMA looks forward to learning more from our readers about their needs and concerns as smart communities that strive daily to provide excellence in how and what they deliver to residents.

Sincerely,

Marc Ott,
Executive Director, ICMA

Chapter 1. Introduction

Roger L. Kemp

Cybersecurity addresses the need for computer security and the protection of an organization's networks and its content or knowledge base. The term describes a dynamic, evolving, and strategic effort to protect an organization's digital systems from things called viruses, bugs, worms, eavesdropping, spoofing, phishing, clickjacking, and social engineering, to name but a few of the threats being faced. There are other security threats, such as preventing the theft of hardware, that local governments must guard against but this report will focus strictly on cybersecurity and the threats it poses. In reality, cybersecurity also refers to protection against as yet unidentified threats.

Computer hackers can steal sensitive and confidential information, such as names and addresses, credit card information, medical information, and related data stored on computers. They can also infect networks with malicious software to destroy network operations. We see it time and again in the corporate world as well as in the government sector—just ask HBO, Sony, Home Depot, Yahoo, and Equifax, not to mention the U.S. Department of Homeland Security and the FBI. The practice is so widespread that Wikipedia maintains a list of hacked businesses along with the cause of the breaches—for instance, poor security, inside job, accidentally published or distributed information, lost or stolen computers, and lost or stolen media.

According to BetaNews, in an article published in 2016, "the total average cost of a data breach is now put at $6.53 million which includes $3.72 million in lost business. . . .The total cost of damage due to cyber attacks is put at $400 million. Forensic investigations can cost up to $2,000 an hour, while the average annual salary of a security engineer is $92,000." [1] In *ITWeb* , Jared van Ast writes that "financial cost can include [people] claiming damages, hiring specialists to assist with repairing the damage, loss in brand value, increased insurance costs, etc."[2] He describes a range of operational costs, including "time lost by employees resolving and repairing; the adjustments required in governance practice, policies, and process; impact to KPI [key performance indicators] metrics and other organizational performance measures, etc." While the dollar estimates of the costs of restoring security vary widely, there really isn't any disagreement about the fact that restoring protection is enormously disruptive.

Which brings us back to the reason for this publication. Even if your organization has not yet experienced a breach, the probable consequences of one are simply too big to ignore. And the probability of remaining protected without having cybersecurity policies, a plan, and established protocols in place and actively updated is not in your favor when data already suggest that breaches and cyber extortion practices are rising.

Before you find your own jurisdiction's security breach in the headlines, consider how a strategic approach can (1) help break down into manageable pieces what may feel like daunting tasks, and (2) protect a public organization, its employees, and the public it serves. Local government managers need to take control and focus on such important matters as:

- **Understanding** what data and information you have on your computer systems that needs protection
- **Encrypting** data and devices, which is the first line of defense to any cybersecurity plan
- **Establishing and implementing** the best cybersecurity practices by putting in place cybersecurity protocols and procedures for all employees in the organization to follow
- **Obtaining and reviewing** cyber insurance policies to be sure that your organization has adequate insurance coverage.

Whenever a local government organization acquires new hardware and software, managers need to ensure that employees are thoroughly educated and trained on cybersecurity protocols and policies. Data breaches frequently happen by accident or mistake, with employees being one of the greatest causes of such breaches.

For example, phishing attacks cause problems when employees indiscriminately click on links or attachments without stopping to consider the source of a tainted e-mail.

Through its participation in smart communities initiatives and the conduct of smart cities and cybersecurity survey research, ICMA has acknowledged the significance of computer networks in effectively delivering services and running government. A hand-in-glove approach is necessary to reduce the risks associated with cyber breaches and incidents that disrupt operations. **This volume sets forth state-of-the-art leading practices that are evolving in this dynamic field. *Cybersecurity: Protecting Local Government Digital Resources* is organized into four segments:**

- **Cybersecurity survey research.** The ICMA/University of Maryland, Baltimore County, 2016 cybersecurity survey of local governments nationwide identified cybersecurity challenges and barriers, the practices of local governments, and the actions that local governments can take to provide better cybersecurity practices and procedures for their organization.

  The constant threat of a cyber attack is the most important problem, though the survey found that many local governments do not know how often they are attacked nor what kinds of attacks are taking place on their organizations' computer hardware and software.

  These data suggest that, on average, local governments in the United States are not undertaking the effort necessary to achieve high levels of cybersecurity on their organizations' computer hardware and software systems.

  The data also suggest a number of straightforward steps that local government managers can implement to improve their organizations' cybersecurity, including acquiring the proper cybersecurity hardware and software and hiring a well-trained staff.

- **Cybersecurity planning.** This chapter focuses on the fact that computer systems represent a critical infrastructure for all local governments in America. After all, when a computer system goes down, it is difficult for the staff to get work done.

  Chapter 3 concludes that local government managers have good reason to fear possible attacks on their computer systems and the negative impact that these can have on their organization and its employees. A proper cybersecurity plan would significantly reduce the threat of attacks and minimize their impact.

  The sections of this chapter include the challenges imposed by cybersecurity, the elements of a successful cybersecurity plan, and the proper way that an organization should respond to a computer breach. Details of this include setting priorities for a computer system's restoration; what steps should be taken to back up data; and the need for all departments, and their employees, to share computer-related resources, both hardware and software.

- **The cloud and enterprise security.** Cloud computing is a form of Internet-based computing that provides shared computer processing resources (e.g., computer networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal management effort. Basically, cloud computing allows users and enterprises with various capabilities to store and process their data in either a privately owned cloud or on a third-party server, in order to make data-accessing mechanisms easier to use and more reliable. Cloud computing relies on the sharing of resources to achieve both coherence and economy of scale.

- **Cybersecurity case studies.** Chapter 5 includes cybersecurity case studies in two U.S. county governments and one city government:
  - DeKalb County, Georgia, has a population of about 740,000, and is one of the largest county governments in the state of Georgia. It is located in the upper portion of the state.
  - Jefferson County, Alabama, has a population of about 660,000, and is the most populated county in the state of Alabama. Jefferson County is located in the center of the state.
  - City of Roseville, California, has a population of about 135,000. The city of Roseville is the largest municipal government in Placer County. It is located in the northern portion of the state, in the Sacramento Metropolitan Area.

  Each of these local government case studies includes background information, as well as details on the planning efforts taken by public officials for computer security, policy development, how their respective programs were funded, how they respond to cyber attacks, organizational collaboration when responding to cyber attacks, staff training, communications, computer monitoring, the recovery process, and lastly, the lessons learned from these processes.

The study's interviewees are listed at the end of each case study so that readers can seek additional follow-up information on any of these cybersecurity processes or retain the lists for future reference.

- **Appendices.** Three appendices are also included in this volume. One is a summary of the cybersecurity survey, and another appendix lists the determinants, which provide an understanding of the impact of the type of local government, its geography, and its population on cybersecurity responses and processes. The third appendix is an annotated resource list.

The subject of cybersecurity is dynamic and evolving, and it affects every local government, in cities and counties, throughout the nation. With this publication ICMA showcases the latest research and leading practices in this changing field. Undoubtedly our collective, shared knowledge about cybersecurity will help local governments strengthen their protection of valued networks and assets. In pursuit of expanding this knowledge base, ICMA Smart Communities Advisory Board members will be working with the ICMA staff during the coming years to determine what other critical cybersecurity best practices our members need to keep pace with the dynamic field of cybersecurity.

Endnotes

[1] Ian Barker, "The Economic Costs of Being Hacked," BetaNews, BetaNews, Inc., February 10, 2016. http://betanews.com/2016/02/10/the-economic-cost-of-being-hacked/

[2] Jared van Ast, "The Cost of Being Hacked," *ITWeb* , April 25, 2016. http://www.itweb.co.za/index.php?option=com_content&view=article&id=151999

Chapter 2. Local Government Cybersecurity in the United States: Survey Reveals Problems and Practices

Donald F. Norris and Laura Mateczun

The 2016 ICMA/University of Maryland, Baltimore County cybersecurity survey is the first-ever nationwide survey of U.S. local governments about their cybersecurity practices and experiences. In this chapter we first briefly discuss the survey methodology; highlight the cybersecurity problems local governments confront and the barriers they must overcome to resolve them; identify actions these governments could take to provide better cybersecurity; and, finally, present conclusions and recommendations that local government managers may find useful in improving cybersecurity.

Method

ICMA sent the survey to the chief information officer in 3,423 local American governments with populations of 25,000 and greater, and 411 responded, for a response rate of 12.0 percent. As Table 1 shows, the results are reasonably representative, although larger local governments and municipalities are somewhat overrepresented, and there is also some regional variation. Beyond this, however, we can have confidence in the survey results because the survey respondents were, for the most part, IT or cybersecurity professionals (83.1 percent) or local government managers (15.8 percent). Thus, expert local government practitioners, who can be expected to "know their stuff," responded to this survey.

Cybersecurity Problems

Clearly, the most important cybersecurity problem that organizations confront is the constant threat of cyber attack. For the purpose of the survey, we defined ***attack*** *as an attempt by any party to gain unauthorized access to any component of your local government's information technology system for the purpose of causing mischief or doing harm.* We used Verizon's definitions of incident and breach (2015 Data Breach Investigations Report). According to Verizon, an ***incident*** is *"Any event that compromises the confidentiality, integrity or availability of an information asset."* A ***breach*** is *"An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."*[1]

A sizeable percentage of local governments (44 percent) reported that they are under attack hourly or daily (26.0 percent and 18.0 percent, respectively). (See Table 2.) Overall, two-thirds (66.7 percent) reported experiencing cyber attacks at least annually. While just over half of local governments reported experiencing incidents, only 9 percent said that they experienced them hourly or daily (4.1 percent and 4.9 percent, respectively). Fewer governments reported breaches (24.2 percent), and fewer still reported them occurring hourly or daily (2.8 percent and 2.2 percent, respectively).

The most troubling results, however, are found in the high percentage of respondents that *did not know* how often they are attacked (27.6 percent) and experience incidents (29.7 percent) and breaches (41.0 percent). A sizeable proportion of local governments also did not know if the frequencies of attacks, incidents, and breaches have changed over the past year (25.8 percent, 27.7 percent, and 35.5 percent, respectively).

Although most local government (88.8 percent) reported that external actors are responsible for

Table 1. Summary Statistics of Respondents

	Number Surveyed	Number Responding	Response Rate
Total	3423	411	12.0%
Population Size			
Over 1,000,000	42	11	26.2%
500,000—1,000,000	98	20	20.4%
250,000—499,999	168	26	15.5%
100,000—249,999	532	63	11.8%
50,000—99,999	939	108	11.5%
25,000—49,999	1644	183	11.1%
Geographic Division			
Northeast	574	46	8.0%
North Central	1048	120	11.5%
South	1148	140	12.2%
West	653	105	16.1%
Type of Government			
Municipalities	1893	267	14.1%
Counties	1530	144	9.4%

Table 2. Frequency

	Attacks	Incidents	Breaches
	n=366	n=367	n=363
Hourly or more	26.0%	4.1%	2.8%
At least once a day	18.0%	4.9%	2.2%
At least once a week	7.7%	5.7%	1.1%
At least once a month	6.6%	10.4%	0.8%
At least once a quarter	4.6%	13.4%	3.3%
At least once annually	3.8%	16.3%	14.0%
Other	5.7%	15.5%	34.7%
Don't Know	27.6%	29.7%	41.0%

attacks on their systems, nearly one-third (31.9 percent) do not know whether attacks were initiated by internal versus external actors. (See Table 3.) One in five governments does not know if breaches to their systems occurred because of phishing or spear phishing attacks (20.5 percent). (See Table 4.) A majority of local governments (58.2 percent) said that they are not able to determine the types of attackers targeting their systems. (See Table 5.) Finally, Table 6 shows that most local governments do not catalog or count attacks (53.6 percent), and about four in ten do not catalog or count incidents and breaches (41.9 percent and 39.9 percent, respectively).

These data strongly suggest that, on average, local governments in the United States are not doing the kind of job necessary to achieve high levels of cybersecurity.

Barriers to Cybersecurity

Table 7 presents results of questions about barriers that might hinder local governments from achieving high levels of cybersecurity. Four barriers are immediately clear. Almost six in ten local governments (58.3 percent) said that inability to pay competitive salaries for cybersecurity personnel constituted a severe or somewhat severe barrier. Adding those that indicated this represents a modest barrier raises the response to 70.5 percent.

Next comes an insufficient number of cybersecurity staff, which 53 percent of governments said constitutes a severe or somewhat severe barrier. Adding respondents who indicated it's a modest barrier raises the response to 74.3 percent. This is followed by lack of adequately trained cybersecurity personnel in the local government, with 46.5 percent saying it is a severe or somewhat severe barrier, rising to 69.6 percent when adding modest barrier. Lack of funds is fourth on the list, with 52.3 percent responding severe or somewhat severe barrier; the level increases to 80.2 percent when adding modest barrier. Clearly, the lack of money underlies the most serious barriers local governments face in their efforts to achieve cybersecurity, at least according to these local expert practitioners.

Funding constraints are also evident from responses to another question (Table 8). Of the five areas of

Table 3. Attack Initiated Externally or Internally

Average Internal		Average External		Don't Know		Total
#	%	#	%	#	%	(n)
226	11.2%	226	88.8%	106	31.9%	332

Table 4. Breaches Due to Spear Phishing Attacks

No Breaches (N/A)		Percentage Known		Don't Know		Total	
#	%	#	%	#	%	#	%
167	45%	128	34.5%	76	20.5%	371	100%

Table 5. Awareness of Types of System Attackers

Is your local government able to determine the types of attackers that attack your system?		
Yes	No	(n)
41.8%	58.2%	368

Table 6. Cataloging or Counting Attacks, Incidents, and Breaches

Attacks		Incidents		Breaches	
n=377		n=377		n=373	
Yes	No	Yes	No	Yes	No
46.4%	53.6%	58.1%	41.9%	60.1%	39.9%

cybersecurity investment, all but one had stayed mostly the same over the past five years. Investment in technology (hardware and software) was the one exception, with 58.5 percent of respondents saying it had increased and only 6.6 percent saying it had decreased. For investments in additional staff, higher staff compensation, training for staff, and policies and procedures, responses ranged from 47.8 percent to 63.0 percent who said it remained about the same over the past five years.

Local government respondents did not feel that the following constitute barriers to achieving high levels of cybersecurity: lack of support from either top elected or appointed officials or local government department managers; the federated nature of local government; and the absence of end-user training. Other potential

Table 7. Barriers to Achieving Cybersecurity

Barrier	n	Not a barrier	Small barrier	Modest barrier	Somewhat severe barrier	Severe barrier	Don't know
Lack of funds	348	7.5%	9.5%	27.9%	18.1%	34.2%	2.9%
Lack of support from top elected officials	345	36.8%	21.2%	20.0%	7.0%	6.7%	8.4%
Lack of support from top appointed officials	334	41.6%	20.7%	16.5%	8.1%	5.1%	8.1%
Lack of support from department managers	345	38.0%	23.5%	20.9%	9.6%	4.1%	4.1%
Lack of availability of trained cybersecurity personnel to hire	345	20.6%	15.1%	21.7%	15.7%	15.7%	11.3%
Inability to pay competitive salaries for cybersecurity personnel	343	10.5%	9.9%	12.2%	21.0%	37.3%	9.0%
Insufficient number of cybersecurity staff	342	8.8%	11.4%	21.3%	17.3%	35.7%	5.6%
Lack of adequately trained cybersecurity personnel in my local government	342	11.7%	13.7%	23.1%	19.6%	26.9%	5.0%
Lack of adequate cybersecurity awareness in organization	341	10.6%	24.3%	31.4%	16.7%	14.1%	2.9%
The federated nature of local government (separation of powers—executive, legislative, judicial)	333	41.7%	13.8%	12.9%	8.4%	9.0%	14.1%
No end-user training at all	340	32.6%	17.9%	20.0%	13.5%	12.1%	3.8%
Some but insufficient end-user training	333	22.5%	24.9%	27.6%	11.4%	8.1%	5.4%
Lack of end-user accountability	342	14.0%	21.6%	23.4%	20.5%	17.0%	3.5%
Too many IT networks/systems within my local government	341	43.7%	1.2%	12.9%	9.4%	7.0%	5.0%
Other	31	22.6%	6.5%	6.5%	6.5%	9.7%	48.4%

barriers received mixed responses, although none rose to the level that suggested that respondents felt that they clearly were barriers.

Two additional barriers could also affect the levels of cybersecurity in complex organizations. These include awareness of the need for cybersecurity and support for cybersecurity among key personnel in these organizations. The data in Table 9 show that that awareness (or, rather, the lack of it) was clearly an issue for these local governments. For example, among all categories of persons, respondents felt that only their top appointed managers were substantially aware of the need for cybersecurity (61.7 percent responded moderately or exceptionally aware, while only 14.0 percent said not aware or slightly aware). Next came department managers (46.5 percent moderately or exceptionally aware and 21.6 percent not aware or slightly aware).

In third place (and nearly tied) were the average end user (34.1 percent moderately or exceptionally aware and 28.8 percent not aware or slightly aware) and elected executives (32.3 percent moderately or exceptionally aware and 27.8 percent not aware or slightly aware). The staffs of elected council members (called "councillors" in the survey; 30.6 percent moderately or exceptionally aware and 31.2 percent not aware or slightly aware) fared considerably better than their bosses, the elected council members (25.6 percent moderately or exceptionally aware but 40.6 percent not aware or slightly aware). The average citizen fared the most poorly (8.4 percent moderately or exceptionally aware and 46.7 percent not aware or slightly aware).

Next, we asked about levels of support that cybersecurity receives from the same personnel in these local governments (Table 10). Once again, the respondents felt that only their appointed managers demonstrated substantial support for cybersecurity (53.8 percent strong or full support and 15.8 percent no or only limited support). Elected executives, department managers, and the staff of elected council members followed, with respondents indicating that about one-third each demonstrated strong of full support and about one-quarter demonstrated no or limited support. The respondents said that slightly less than one-quarter of end users demonstrated strong or full support and about one-third demonstrated no or limited support. Once again, the average citizen came in last, with only one in 14 demonstrating strong or full support and about four in ten demonstrating no or limited support.

These data should be of concern to local governments because they do not suggest sufficiently high levels of awareness of the need for cybersecurity or support for cybersecurity among key personnel in (and outside of) local governments. In order to achieve high levels of cybersecurity in these organizations, leaders need to demonstrate their personal commitment to it and take other actions (some of which we discuss in the following section) to improve both awareness of and support for cybersecurity.

Actions to Improve Cybersecurity

Organizations have at their disposal a number of actions and practices to help improve their levels of cybersecurity. We asked these local governments about fourteen of them (Table 11). Strikingly, for many of these actions, a sizeable percentage of local governments responded that they never take them. These included, in order of frequency:

1. cybersecurity awareness training for citizens (71.4 percent never take them, with 20.6 percent saying that they do not know)
2. cybersecurity awareness training for contractors (61.9 percent never and 19.9 percent do not know)
3. cybersecurity awareness training for local elected officials (50.1 percent never and 13.8 percent do not know)
4. forensic services after incidents or breaches (42.9 percent never and 20.7 percent do not know)
5. cybersecurity exercises (40.8 percent never and 11.8 percent do not know).

When asked about other actions, by contrast, local governments appear to be doing a better job. The great majority (77.5 percent) undertakes scanning and testing at least annually, and 38.2 percent scan and test at least monthly. Nearly two-thirds (63.3 percent) undertake risk analysis at least annually, and a similar percentage (63.5 percent) conducts technical security reviews at least annually. Somewhat less than half (48.2 percent) reported conducting cybersecurity awareness training for non-cyber IT personnel at least annually.

Nearly six in ten (59 percent) provide cybersecurity staff training at least annually, although one in five

Table 8. Cybersecurity Investment Changes Over the Past Five Years

	n	Decreased Greatly	Decreased Slightly	About the Same	Increased Slightly	Increased Greatly	Don't Know
Technology (hardware, software, etc.)	347	2.3%	4.3%	31.1%	35.7%	23.1%	3.5%
Additional staff	345	5.2%	6.4%	55.1%	20.6%	8.7%	4.1%
Higher staff compensation	343	3.2%	7.9%	63.0%	18.4%	1.5%	6.1%
Training for staff	345	4.1%	8.7%	49.0%	25.8%	7.2%	5.2%
Policies and procedures	345	2.3%	5.2%	47.8%	31.0%	7.5%	6.1%

Table 9. Awareness of Cybersecurity

Unit	n	Not aware	Slightly aware	Somewhat aware	Moderately aware	Exceptionally aware	Don't know
Department managers	362	2.5%	19.1%	32.3%	33.7%	8.8%	3.6%
Elected executive	313	7.7%	20.1%	26.2%	24.6%	7.7%	13.7%
Elected councilors/ commissioners	359	9.7%	30.9%	25.5%	20.9%	4.7%	7.2%
Staff of elected councilors/commissioners	324	7.1%	24.1%	26.2%	24.4%	6.2%	12.0%
Top appointed manager	342	2.9%	11.1%	19.0%	42.7%	19.0%	5.3%
The average end user	361	5.0%	23.8%	33.2%	29.1%	5.0%	3.9%
The average citizen	357	10.6%	36.1%	24.4%	7.6%	0.8%	20.4%

Table 10. Support for Cybersecurity

Unit	n	No support	Limited support	Moderate support	Strong support	Full support	Don't know
Department managers	354	4.2%	22.6%	34.7%	21.2%	12.1%	5.1%
Elected executive	284	5.3%	19.7%	26.1%	16.2%	19.4%	13.4%
Elected councillors/ commissioners	349	6.3%	25.5%	28.4%	14.3%	16.0%	9.5%
Staff of elected councilors/commissioners	305	7.2%	21.6%	26.6%	15.1%	15.7%	13.8%
Top appointed manager	329	3.3%	12.5%	23.7%	25.8%	28.0%	6.7%
The average end user	351	6.8%	28.2%	36.8%	16.0%	6.0%	6.3%
The average citizen	341	18.5%	24.6%	16.7%	5.0%	2.3%	32.8%

(20.9 percent) provides no such training. Similar fractions (58.4 percent) provide cybersecurity awareness training for cybersecurity staff, although 25.1 percent provide none; and 58.3 percent provide cybersecurity awareness training for non-cyber IT staff, although 23.3 percent provide none. Last, almost five in ten (48.8 percent) provide end-user training, although 29.5 percent provide none.

We also wanted to know if local governments had developed certain policies that could enable the achievement of high levels of cybersecurity and, whether, if these policies had been adopted, they were effective (Tables 12 and 13). First, we asked about the adoption of seven specific policies. Of the seven, large majorities of local governments had adopted only three: (1) rules regarding how passwords can be made (77.4 percent had developed); (2) requirements about the frequency that end users must change passwords (77.1 percent); and (3) policies on employee use of personal electronic devices on local government IT systems (61.8 percent).

A fourth policy achieved nearly majority adoption: (4) cybersecurity plans (47.7 percent, although 52.3 percent had not developed such plans). The remaining policies had been adopted by only around one-third of local governments: (5) standards for vendors of

Table 11. Actions Taken to Improve Cybersecurity

Action	n	Never	At least monthly	At least quarterly	At least annually	At least every 2 years	Don't know
Scanning and testing	351	7.4%	38.2%	19.4%	19.9%	10.0%	5.1%
Risk assessment	352	13.4%	9.9%	12.5%	40.9%	16.2%	7.1%
Technical security review	351	12.0%	8.5%	16.8%	38.2%	16.5%	8.0%
Cybersecurity exercises	348	40.8%	3.7%	6.3%	25.0%	12.4%	11.8%
Audit of our cybersecurity practices	345	26.7%	2.6%	5.5%	38.6%	17.7%	9.0%
Forensic services after incidents or breaches	217	42.9%	8.8%	6.9%	17.5%	3.2%	20.7%
Cybersecurity staff training	349	20.9%	8.6%	10.3%	40.1%	12.0%	8.0%
End-user training	346	29.5%	5.8%	9.5%	33.5%	11.8%	9.8%
Cybersecurity awareness training for local government employees	350	31.7%	3.1%	10.0%	35.1%	10.9%	9.1%
Cybersecurity awareness training for local government elected officials	347	50.1%	2.6%	3.2%	21.3%	8.9%	13.8%
Cybersecurity awareness training for local government information technology personnel (not including cybersecurity personnel)	347	23.3%	10.7%	10.1%	37.5%	11.0%	7.5%
Cybersecurity awareness training for local government cybersecurity personnel	339	25.1%	11.5%	13.0%	33.9%	7.1%	9.4%
Cybersecurity awareness training for citizens	339	71.4%	1.2%	0.3%	5.0%	1.5%	20.6%
Cybersecurity awareness training for contractors	341	61.9%	2.6%	1.8%	11.7%	2.1%	19.9%

cloud-based services (35.7 percent); (6) written plans for recovery from breaches (33.7 percent); and (7) written cybersecurity risk management plans (33.1 percent).

Overall, these data suggest, once again, that local governments are not taking sufficient actions to properly protect their cyber investments.

Next we asked respondents to rate the effectiveness of those policies that had been developed. We asked respondents to rate the policies' effectiveness as very low, low, average, high, or very high. Although large pluralities of respondents rated the effectiveness of most policies as average, sizable numbers rated them as ineffective, and in only two cases did majorities of respondents rate policies as highly or very highly effective. In order of frequency of highest ratings, these policies were:

Table 12. Adoption of Cybersecurity Policies

	n	No, not developed	Yes, developed
Formal, written cybersecurity policy, standards, strategy, or plan	346	52.3%	47.7%
Formal, written cybersecurity risk management plan	344	66.9%	33.1%
Formal, written plan for recovery from breaches	341	66.3%	33.7%
Formal, written rule(s) regarding how passwords can be made	349	22.6%	77.4%
Formal, written requirement for end users to change passwords periodically	349	22.9%	77.1%
Formal, written policy governing the use of personally owned devices by governmental officials and employees	346	38.2%	61.8%
Formal, written cybersecurity standards for contracts with vendors for cloud-based services	339	64.3%	35.7%

Table 13. Effectiveness of Adopted Cybersecurity Policies

	n	Very low	Low	Average	High	Very high	Don't know
Formal, written cybersecurity policy, standards, strategy, or plan	151	13.2%	17.9%	46.4%	17.2%	5.3%	2.9%
Formal, written cybersecurity risk management plan	103	14.6%	16.5%	44.7%	19.4%	4.9%	8.4%
Formal, written plan for recovery from breaches	106	14.2%	14.2%	44.3%	21.7%	5.7%	8.1%
Formal, written rule(s) regarding how passwords can be made	246	6.9%	5.3%	32.1%	37.4%	18.3%	4.1%
Formal, written requirement for end users to change passwords periodically	248	6.0%	5.6%	29.0%	37.1%	22.2%	11.3%
Formal, written policy governing the use of personally owned devices by governmental officials and employees	190	10.0%	11.1%	38.9%	29.5%	10.5%	9.0%
Formal, written cybersecurity standards for contracts with vendors for cloud-based services	112	14.3%	9.8%	41.1%	25.0%	9.8%	5.6%

1. requirement for end users to change passwords—59.3 percent highly or very highly effective versus 11.6 percent very low or low
2. rules about how passwords can be made—55.7 percent high/very high and 12.2 percent very low/low
3. policies on employee use of personal electronic devices on local government IT systems—40.0 percent high/very high and 21.1 percent very low/low
4. cybersecurity plans—34.8 percent high/very high and 24.1 percent very low/low
5. standards for vendors of cloud-based services—27.4 percent high/very high and 28.4 percent very low/low
6. written plans for recovery from breaches—24.3 percent high/very high and 31.1 percent very low/low
7. written cybersecurity risk management plans—22.5 percent high/very high and 31.1 percent very low/low.

Thus, not only have relatively few local governments developed policies that would help them achieve high levels of cybersecurity, few that have developed such policies rate them as highly or very highly effective.

Conclusions and Recommendations

The portrait that these survey data present is one of local governments facing serious cybersecurity threats while appearing unable to provide the highest levels of cybersecurity. We strongly suspect, although we have not yet verified this with more sophisticated statistical analysis of the data, that less populous local governments and those facing greater budgetary constraints are likely among those with the poorest cybersecurity capabilities and records.

What can managers do to improve the security of their local governments against cyber threats? The top three actions that the respondents to the survey recommended were greater funding for cybersecurity, better cybersecurity policies, and greater cybersecurity awareness among employees in their local governments. (See Table 14.) The next two most frequently

Table 14. Top 3 Improvements to Cybersecurity.

	1	2	3	Total
Greater funding for cybersecurity	76	37	26	139
Better cybersecurity policies	46	36	38	120
Greater cybersecurity awareness among employees in my local government	42	29	48	119
Improved cybersecurity hardware	35	26	22	83
More cybersecurity personnel	26	37	23	86
More end-user training	22	32	33	88
More training for cybersecurity personnel	21	24	28	73
The ability to pay competitive salaries for cybersecurity personnel	15	30	20	65
Greater end-user accountability	13	18	34	65
Better enforcement of existing cybersecurity policies	11	26	17	54
Greater support from top elected officials for cybersecurity	9	9	13	32
Greater support from department managers for cybersecurity	5	13	12	31
Greater support from top appointed officials for cybersecurity	7	3	10	21
Consolidation of our numerous IT networks/systems	3	3	7	14

mentioned were improved cybersecurity hardware and more cybersecurity personnel.

We certainly agree with those actions but believe that improving cybersecurity also requires managers to create and maintain cultures of cybersecurity within their local governments. This must be done in cooperation with the local elected officials, IT and cybersecurity staff, department managers, and end users. Everyone must understand the importance of cybersecurity and their individual roles in maintaining it, and all must be held accountable for their online behavior and actions.

To create and maintain a culture of cybersecurity, local governments must adopt and implement proper policies, procedures, and practices. These include, but are not limited to, those discussed above (see Tables 11 and 12). In addition, local governments must establish clear and transparent means to hold all end users (regardless of their location in the hierarchy) strictly accountable for their actions regarding cybersecurity. At the same time, end users must receive adequate cybersecurity training that is updated periodically. In addition, appropriate penalties must be enforced (up to and including termination of employment for repeat offenders).

The good news is that, for the most part, local governments can implement policies, procedures, and practices to improve cybersecurity without spending a lot of money. However, there are other actions, without which there is little hope of achieving high levels of cybersecurity, that will require funding. First, managers must ensure that their local governments have the proper cybersecurity technology (hardware and software) that is capable of detecting, cataloging, and preventing attacks, incidents, and breaches, as well as detecting the exfiltration of data and information.

Second, managers must see to it that their local governments hire and retain the proper number of well-trained IT and cybersecurity staff. A chief information security officer (CISO) from a large local government told us that his organization had two cybersecurity engineers, but that "Google has 2,000." If the funding and staffing are not available internally, managers should consider outsourcing cybersecurity. Another option might be for managers to have their IT and cybersecurity staffs look into cybersecurity insurance. Other CISOs have told us that the mere act of applying for such insurance requires a risk management exercise that will be valuable in identifying cyber weaknesses that then can be addressed.

We would urge all to understand that cybersecurity is not, nor should it ever be, the sole or even primary responsibility of the IT and cybersecurity staff in their organizations. While technical staff are essential to cybersecurity, at the end of the day, elected and appointed officials have a significant responsibility for cybersecurity in their local governments—a responsibility that they should embrace and from which they should lead.

Endnote

1. Verizon, *2015 Data Breach Investigations Report*, https://media.scmagazine.com/documents/117/verizon_dbr_29210.pdf

Chapter 3. A Plan for Cybersecurity

Cory Fleming

At Issue

Computer systems represent critical infrastructure for all local governments. When a computer system goes down, it's difficult for staff to get work done. Recreating data stolen or lost in a cyber attack is time-consuming and labor intensive. With stories about cybersecurity attacks, security breaches, and information leaks popping up in the news on nearly a daily basis, local government managers have good reason to fear possible attacks to their computer systems and the havoc the attacks could cause.

All organizations—big and small—are vulnerable to attacks. Instituting cybersecurity programs and procedures is a bit like buying insurance from a risk management standpoint: You hope you never encounter attacks or breaches but you want to be prepared if you do. The challenge is to stay ahead of technology that continually morphs into new threats. At the same time, managers cannot be concerned only about the most recent attack or threat. They must look at the big picture to determine what it takes to always be operating in a secure environment. Consideration needs to be given to how managers can respond to keep systems safe while not breaking their budgets; how local governments can retain qualified IT staff when private sector salaries are significantly higher; and for small community managers who also wear the hat of chief information officer (CIO), how they can stay abreast of trends and choose the most practical option.

Challenges

Workforce. Multiple studies have found that the lack of skilled IT personnel in the public sector is a significant problem. High salaries in the private sector make it difficult to attract IT talent to public sector positions and then also retain them, especially those individuals specializing in cybersecurity. Further aggravating the situation, leadership within the IT public sector is aging and many talented individuals have begun retiring in force. "A slow but persistent drain on human resources looms large, with many states reporting that 20 to 60 percent of their IT employees are nearing or at the age of retirement," according Derek Johnson, a state and local analyst with Deltek.[1]

An available workforce is simply not there for local governments to hire. "Thirty-five percent of organizations have open security positions that they are unable to fill and 53 percent say it can take as long as six months to fill one need, according to 'The State of Cybersecurity: Implications for 2015,' a study by ISACA," reports Marc van Zadelhoff of IBM Security.[2]

Budgeting. Cybersecurity is a critical issue for many communities that may not have the necessary funding or resources available to protect computer systems. While Noelle Knell reports in *Government Technology* that "[c]ities are expected to spend $30.9 billion on IT in 2017...and counties $22 billion,"[3] Paul Lipman, CEO of iSheriff, points out that "[t]he typical state or local government agency spends less than 5% of its IT budget on cybersecurity, compared to over 10% in the typical commercial enterprise."[4]

However, many security measures are simple and low-cost, such as following good password practices, changing system passwords on a routine basis, keeping browsers and operating systems updated, and using two-factor authentication systems (a passcode and a security question) where possible. In addition, training and education—helping staff understand what to watch for to prevent attacks—can help ward off new threats.

Plan Elements

Research and Needs Assessment. Research on current technology solutions is crucial for understanding the wide range of products available and how well those products can be expected to perform over time. Local governments should avoid quick fixes and one-off solutions. Instead, staff should research how products can be integrated with existing systems to produce better results.

Likewise, a needs assessment can help IT professionals determine what their requirements for technology solutions should be. A needs assessment begins with inventorying legacy systems currently being used and identifying where security gaps may exist. For example, is the credit card payment system protected from hackers trying to enter through the city's website? Local governments need to understand their cyber vulnerabilities and what it takes to mitigate those risks.

Policies and Procedures. Local governments need to develop written policies and procedures on how the organization will protect its computer systems. Buying software solutions or electronic devices alone will not protect a system. Employees must understand that human error plays a substantial role in many security breaches. Clicking on suspicious links in e-mails or not using a secure passcode to lock a computer screen when away from the computer exposes the organization's system to unneeded risk. While people are human and make mistakes, routine reminders of the organization's policies and procedures keep security measures at the forefront of staff concerns.

Roles and Responsibilities. Successful recovery from a cyber attack or other security incidents involving local government computer systems requires planning and preparation in the same way that recovery from natural and human-made disasters do. When employees know, *before* an incident occurs, who is responsible for what tasks and what actions will be top priorities, the response goes more smoothly and quickly. Establishing good working relationships before an event is helpful when determining what resources are available and which staff have needed skill sets to respond.

Training and Education Programs. As noted earlier, the number of openings in the cybersecurity field far outpace the number of trained professionals available to fill those positions. This general lack of IT talent makes it imperative for local governments to invest in training and education for existing staff. The level of training needed will vary among individuals, but team members need to be aware of system vulnerabilities, how and where they should look for potential risks, and the tools available to protect systems. At a minimum, all employees need to know and follow recommended safety standards.

System Integration. Computer systems, devices, and other technology solutions need to work together to achieve maximum protection. Often, however, staff purchase a one-off solution designed to solve a specific issue, but the solution won't work with related issues. Consider the relationship between an app for identity protection and one for theft protection. Both solutions provide a certain level of protection, but if the apps are integrated, the level of protection is far greater. "Cybersecurity needs to be integrated throughout an institution as part of enterprise-wide governance processes, information security, business continuity, and third-party risk management," according to the Federal Financial Institutions Examination Council.[5]

Security Audits. All local governments need to conduct regular security audits to determine what data may be at risk and enable staff to understand where threats and vulnerabilities exist in the system. Internal controls for IT are often overlooked, including, for example, limiting the number of staff who have access to business operations data, establishing security and privacy policies for staff, or maintaining password-protected locations within a system. Adherence to simple security practices like these ensures data integrity and protects the organization's systems by limiting opportunities for breaches. By identifying what data assets an organization maintains and classifying the importance of that data, IT staff can act to protect against those risks. Security audits also provide a good starting point for conducting a needs assessment to support the development of a cybersecurity plan. A needs assessment defines the tasks and activities that should take place to move a local government from "ready for the status quo" to "ready for the unknown."

Monitoring. Local governments are capturing and maintaining increasing amounts of data every year due to sensors, the Internet of Things (IoT), body-worn cameras, and other new technologies. The new data make it possible for local government professionals to analyze data and make better management and policy decisions based on data. Increased data sharing within and outside a local government organization represents new opportunities to adopt smart community management practices that range from developing smarter deployment of staff for routing lawn and turf management to the use of drones to collect high-resolution images for marketing business and industrial sites for development.

New data and sharing of that data, however, also open new opportunities to transmit viruses and could make a local government vulnerable to other malicious activity. Monitoring is used for threat detection, but risk specialists at Deloitte note that monitoring should be used to “proactively identify those activities most detrimental to the business and support mitigation decisions.”[6]

Continuity of Operations. Public safety officials have routinely developed plans for the continuity of operations should a disaster hit their community. Just as leaders map out evacuation routes to prepare for flooding or where to set up shelters during a hurricane, so too must they consider which data and computer systems are most critical for daily operations or how they can rebuild systems as quickly as possible in the event of a cyber attack. Backup plans for what to do in the event of a digital attack are as important for keeping a community operational as are those for roads and shelters during a storm.

Communications. Communication is critical when any emergency or disaster hits. Local government managers need to be prepared to communicate using different channels during a natural disaster. During a cyber attack, the need to have access to multiple forms of communication is even more relevant. Email, texts, instant messages, and other electronic channels may be shut down during an incident. In addition to being physically able to communicate and coordinate within the organization, local governments also need to be prepared to brief elected officials, the news media, and the public about what happened, how it was contained, and what, if any, damage was sustained. A clear, concise, and accountable message after an event will go a long way to reassuring stakeholders that their personal data are protected.

Responding to a Breach

Setting Priorities for Systems Restoration. Each community will have different priorities for systems restoration. For almost all communities, however, systems delivering critical citizen services—such as health (a county hospital) or safety (police communications)—will be first among identified priorities. Police, fire, and emergency medical personnel need to be able to communicate and access their data quickly.

Backup Data. Most local government organizations routinely back up data in their systems, but often employees don’t back up their local drives to prevent loss of programs in the event of an attack. Field crews using mobile technology such as smartphones and tablets should be routinely backed up, saving both data as well as program files. Employees who use laptops should also perform full backups on their machines daily.

Sharing Resources. Unlike the private sector, which must contend with business competition, local governments and other public agencies can and should work together. Whether it is sharing leading practices or splitting costs to purchase necessary software, local governments have options available to them that businesses don’t.

Assessment and understanding of your organization’s levels of cybersecurity take the same kind of planning that you invest in budgeting and strategic planning. The old adage—“By failing to prepare, you are preparing to fail”—is true. Strategic planning enables local government leaders and staff to prepare for a more secure future.

Endnotes

[1] Derek Johnson, “State, Local Governments Turn Attention to Cybersecurity Capabilities,” *The Washington Post*, April 26, 2014. https://www.washingtonpost.com/business/capitalbusiness/state-local-governments-turn-attention-to-cybersecurity-capabilities/2014/04/04/8527c4b0-b912–11e3–899e-bb708e3539dd_story.html?utm_term=.b1dca4b314de

[2] *Marc van Zadelhoff, “Four Big Cyber Security Challenges (and How to Overcome Them),” Forbes*, May 14, 2015. https://www.forbes.com/sites/ibm/2015/05/14/four-big-cyber-security-challenges-and-how-to-overcome-them/#5771430e5867

[3] Noelle Knell, “IT Spending in State and Local Government: What Does 2017 Hold?”, *Government Technology*, March 20, 2017. http://www.govtech.com/budget-finance/IT-Spending-in-State-and-Local-IT-What-Does-2017-Hold.html

[4] Lipman, Paul, “The Cybersecurity Challenges Facing State and Local Governments,” *infosecurity*, August 19, 2015. https://www.infosecurity-magazine.com/opinions/cybersecurity-challenges-state/

[5] Federal Financial Institutions Examination Council, *FFIEC Cybersecurity Assessment Tool*, May 2017. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf

[6] Christopher Stevenson, Andrew Douglas, Mark Nicholson, and Adnan Amjad, “From Security Monitoring to Cyber Risk Monitoring: Enabling Business-aligned Cybersecurity,” *Deloitte Review*, Issue 19, July 25, 2016. https://dupress.deloitte.com/dup-us-en/deloitte-review/issue-19/future-of-cybersecurity-operations-management.html

Chapter 4. The Cloud and Enterprise Cybersecurity: Leveling the Playing Field

Microsoft

Intelligent security is something we all strive for in the ever-evolving world of cyber threats to the enterprise. The status quo is no longer able to keep up with the pace at which threats morph and replicate themselves across the globe. The "bad guys," in many cases, are better funded and staffed with greater cyber expertise than the agencies which they target. Another growing concern is that the networks from which these global assaults are launched are almost always larger and more resilient than the network they are attempting to compromise. What is a CISO to do? What is the hope of the enterprise when the traditional methodologies of cyber security fail or are prone to compromise themselves? The answer? Enterprises must go global with their effort to not just defend but fight back.

Is an organization able to find the signal in the noise of data points? This we know: attackers aren't going to wait for security software to catch up. Industry reports show advanced cyber attacks can go undetected for approximately 200 days. In today's threat environment, organizations need intelligent security solutions that continually evolve to keep up with the latest threats as they emerge.

Using machine learning to detect advanced cyber attacks, a progressive, data-driven model of cybersecurity has emerged to speed up detection time and reduce risk. Where is this model playing out, one might ask? The model is alive, well, and delivering results in the Microsoft cloud.

Modus Operandi: The Advanced Attack at Work

When security professionals detect a breach, it's almost certain that the attacker has been active in the victim's environment for some time. But how long?

For many in the industry, "200 days" has been accepted as a standard to frame the average. But this "standard" is also problematic for a couple of reasons.

First, that's a long time. It's roughly six-and-a-half months that a sophisticated cyber attacker or syndicate has been at work inside the system. What does an advanced attack do for those 200 days after it's gained entry to the network? Today, attackers employ a mix of methods, using traditional techniques alongside new ones as they constantly explore ways to exploit both people and technologies. The longer an undetected attack lives in your system, the more intel it can glean, underscoring the importance of early detection. Throughout this dark and exposed time, an organization's sensitive data and intellectual property have been potentially exposed, moving closer to inevitable compromise.

The fear of what goes on during those 200 days has made this statistic a yardstick for CISOs, CSOs, and even CEOs. Today, companies, security professionals, and the tech industry at large are thirsty for new, more advanced security measures to drive that number down.

Second, CISOs and CSOs know that the number of days isn't the most important element of a breach. So, as a practical matter, "200 days" is just a milestone, a figure used to measure and discuss the industry's progress. Even one day is too long, and by the time it is discovered, it's always too late. Shrinking that number to zero is the ultimate goal.

To do that, organizations need a more intelligent approach to detect threats earlier and turn the tide against sophisticated cyberattacks. This chapter is designed to give readers a glimpse into how advanced threats are working to compromise sensitive information, and how the advanced computing power of the cloud, combined with data science and human experts, can help reduce the time it takes for an organization to detect an attack.

Attackers that deploy advanced exploits are a constant concern for the small agency or the largest enterprise, and repercussions of an attack go well beyond the initial costs of a breach. Highly skilled, well-funded, and constantly evolving, these perpetrators have motives that range from theft, to industrial espionage, to full-blown nation-state attacks.

Risk: Exposure Is Steeper than Ever

First, there are the financial concerns. Today, the many malicious actors and authors that utilize advanced attacks are looking to profit from their efforts. It's no surprise, then, that the damages keep going up.

In 2015, a new threshold was reached when a sophisticated attack ring successfully breached more than one hundred banks across thirty countries, with losses estimated to exceed $1 billion. Because of the heightened risk, cyber insurance policies are becoming a new operating expense for many companies, with premiums for that emerging offering set to triple by 2020, approaching $7.5 billion.

There are also the less quantifiable and potentially costlier scars that successful cyberattacks leave, such as damaged brands, wary customers, stagnant growth, and compromised diplomatic relations. While not directly attributable to a dollar sign, these impacts can have lasting negative effects on an organization: driving down customer loyalty, driving up public skepticism, and ultimately impacting security operations staff who must be held accountable for breaches.

Other attacks are motivated not by financial incentives, but by a quest for sensitive information. Take STRONTIUM, for example. STRONTIUM is a well-known activity group whose targets include government bodies, diplomatic institutions, journalists, and military forces. It is not after money and doesn't care about size of a target. It is after the most sensitive data it can find. Similarly, the Red October attack group uncovered in 2013 was found to have been infiltrating government and diplomatic institutions for at least five years.

Although it sounds like something out of a spy novel, it's a real issue. Unseen costs of security breaches are something that even two decades ago would sound like the plot of a sci-fi story. With so much at stake, it's no wonder that budgets are increasing, and companies are hungry for new solutions to address the growing problem of advanced cyber attacks.

Nearly 80 percent of cyber attacks begin with a good old-fashioned con job, using spear phishing attacks with compelling ruses to get users to compromise their information. But as security provider McAfee noted, more sophisticated attacks are on the rise, including new integrity attacks that can modify internal processes and reroute data as it flows through the network.[1] (This was the technique used in that $1-billion bank heist.) Attackers continue to evolve with new forms of malware that can better hide from detection or erase themselves altogether. Attack vectors are also changing: No longer content with targeting PCs and servers residing in the corporate headquarters, attackers look to compromise satellite offices; workers' home computers; and even the software inside of cell phones, wearable devices, and automobiles.

The Cyber Kill Chain: A Basic Understanding

Breaches generally involve six clear phases, known in the security intelligence community as the Cyber Kill Chain®, a phrase trademarked by Lockheed Martin. These phases can occur sequentially, in parallel, or in a different order altogether, and each also offers an opportunity to gain intelligence to defeat attackers.

A Proactive Security Model: Staying One Step Ahead

Due to the stealth nature of advanced attacks, companies must shift to a more proactive security model that focuses on improving their ability to sniff out the attacker and stop him in his tracks.

Whereas the traditional model of enterprise security began with protecting the network perimeter, experts now suggest a more proactive approach that begins with detection enabled by robust security analytics. This model promotes a constantly improving cycle, as pre-breach defenses are continually improved with new intelligence from post-breach detection and response.

For the past few years, CISOs and CSOs have been working to make this shift by implementing security intelligence measures that use data and analytics in an effort to rapidly detect the next attack and improve defenses overall. This includes steps such as the following:

Reconnaissance

The attacker explores his target. This may involve technical procedures or simply browsing the company's web site. It often goes undetected, but the potential is there to correlate seemingly benign behaviors for advanced warning of an attack.

Weaponization

The attacker creates a shell to hide a malicious payload. It's not always possible to detect the attack's particular weaponization vehicle, but once discovered and reverse-engineered, it becomes a clear footprint for similar attacks later on.

Delivery

The attacker infects the system with malicious code, or dupes a user into downloading it. This is the critical phase where the attacker gains entry and begins to do his work.

Exploitation

The code compromises the system. Sometimes the delivered code begins immediately to do the attacker's bidding. Other times the attack takes on multiple phases, such as when the initial package begins downloading other code, exposing itself to network alerts.

Command and control (C2)

The attacker and the code work together to exploit the system. This may take the form of lateral movements designed to acquire higher-value credentials, or directly exploring the network to find the targeted data assets.

Actions on intent

Sensitive data is taken. At this point, the attack has been successful. Whether it's your customers' financial information, top-secret documents, or the blueprints for your next-generation product, it's now in the attacker's hands.

Source: Lockheed Martin

- Investing in advanced security software and secure hardware
- Training employees on security imperatives and risks
- Deploying a security intelligence event management (SIEM) solution
- Subscribing to (often multiple) threat intelligence feeds
- Developing processes to correlate threat data, and even hiring data scientists to analyze it.

Thus far, these tools and processes have comprised the bulk of the industry's response to advanced attacks. Like many early-stage efforts in the tech industry, they have had mixed results.

It's not that they aren't effective. Mandiant's 2016 M-Trends report shows that when companies are successful at detection using their own systems, the time of an advanced attack's residency is cut drastically. But there are also complaints—including the expense, cumbersome integration, and the inefficient manual process of correlating threat data and feeding it into the system. And once everything is in place with the SIEM, there's another problem—noise. There are simply too many alerts, too much data, for even the most advanced enterprises to make sense of it all. If the goal of all these efforts is to shorten those 200 days to near real time, then cutting through the noise has become a major roadblock, and part of what keeps detection a (costly) step behind.

To keep up with advanced attacks, organizations should continue investing in their SIEMs and associated process. Only the cloud can offer next-generation protection, detection and remediation at the scale needed today—including alert mechanisms integrated through platform sensors—in a way that constantly evolves to improve protections with true security intelligence.

Improving Detection: The Importance of Clear Signal

Reducing the time it takes to detect an attack presents enterprises with a new dilemma: having too much security-related data to process yet still not having enough information to separate the signal from the noise and understand an incident quickly.

The challenge here is not just sheer volume, but also separation. Many indicators of attack either seem innocent on their own, or are separated by industries, distances, and time frames. Without clear insight into the whole data set, early detection becomes a game of chance. Even the largest enterprises are facing these limitations:

- Real threat intelligence requires more data than most organizations can acquire on their own.
- Finding patterns and becoming smarter in that huge data pool require advanced techniques like machine learning along with massive computing power.
- Ultimately, applying new intelligence so that security measures and technologies constantly improve requires human experts who can understand what the data are saying, and take action.

This is where Microsoft is working to turn the tide. As a platform and services company, Microsoft's threat and activity data come from all points in the technology chain, across every vertical industry, all over the world.

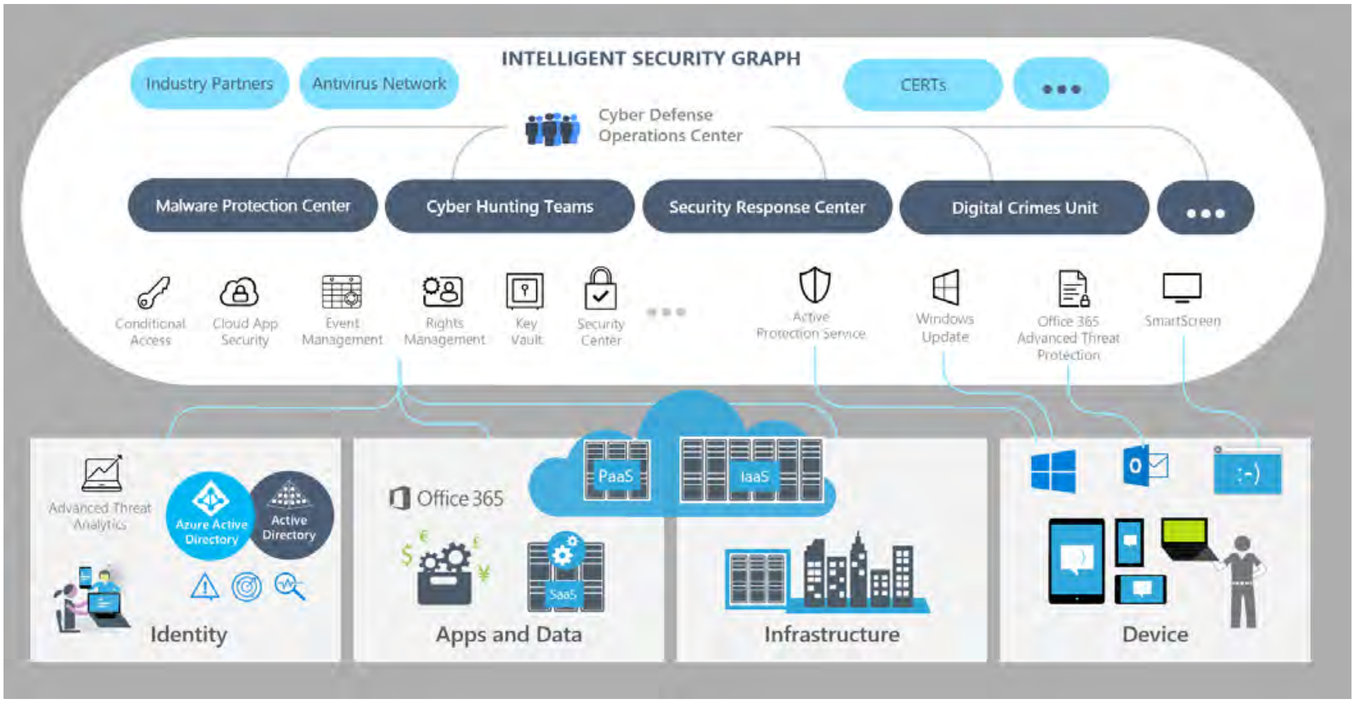
Microsoft's security products and cloud technologies are designed to work together to report malicious threat data as problems occur. This provides a "flight data recorder" that enables us to diagnose attacks, reverse-engineer advanced threat techniques, and apply that intelligence across the platform. The picture below illustrates advanced machine learning and intelligence gathering techniques working with traditional security methodologies to provide a holistic, dynamic, flexible, and easily manageable enterprise cybersecurity posture. This approach leverages cloud-based technologies, which a customer simply would be unable to duplicate on its premises at the scale required to be of value.

From Months to Minutes: Applied Analytics and Continuous Improvement

For nearly two decades, Microsoft has been turning threats into useful intelligence that can help fortify its platform and protect customers. Since the Security Development Lifecycle born from early worm attacks like Blaster, Code Red, and Slammer, to modern security services woven into our platforms and services, the company has continually built processes, technologies, and expertise to detect, protect, and respond to evolving threats. As our digital environment increasingly dominates day-to-day lives, the importance of providing strong data protection and cybersecurity is apparent. From small towns to large cities, all local governments are susceptible to cyber attacks and need to take proactive steps to prevent and mitigate damage from attacks.

Endnote

1. McAfee Security, *"McAfee Labs 2017 Threats Predictions November 2016"* https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf



Source: Microsoft

Chapter 5. Cybersecurity Case Studies

Cory Fleming

DeKalb County, Georgia—Community Profile

- **Population:** 740,321 (fourth largest county in Georgia)
- **Median Household Income:** $51,376
- **Cybersecurity Budget:** operations budget $650,000 annually; capital budget varies annually between $250,000 to $500,000 depending on need
- **FTEs Working in Cybersecurity:** 4

Background

Cybersecurity became a mainstream concern among all industries, not just local governments, in the late 1990s. Robert Morris created the first "worm" in 1998, shutting down much of the Internet with the first known "denial of service" attack on record. The Melissa and "I Love You" viruses infected tens of millions of PCs and caused havoc with email systems around the globe.

Since that time, cyberattacks have become much more commonplace and increasingly destructive across every industry. And with the continuing growth of the Internet and dependence on computers, cybersecurity became a concern not only of DeKalb County but of all local, state, and federal governments. It has become incumbent for IT departments in all industries to be proactive and not reactive in preparing for breaches. Part of being proactive means having a plan and structure along with organization-wide policies, procedures, training, and communication.

Planning for Security

John Matelski, DeKalb County's chief innovation and information officer (CIIO) and director of innovation and technology (IT), explained that the team leadership in the IT department for DeKalb County has been together for five years, and it has done everything possible to shore up all layers of security across the organization. Key components of the county's cybersecurity's plan include:

- Data and intellectual property
- Infrastructure defenses
- Identity management
- User management.

Responsibility for cybersecurity resides in the county's IT department. In DeKalb County, IT stands for innovation and technology, with the department not only handling the technology infrastructure but also taking the lead in encouraging greater innovation and technology education within the county. The IT department has always taken the lead in developing an annual cybersecurity plan for the county as well as collaborating and coordinating on security matters with all county departments. Matelski explains that it is necessary to look at all systems in the organization in a holistic fashion when it comes to the issue of cybersecurity.

DeKalb County has 30 departments and agencies and 6,500 employees. The IT department functions largely as the hub in a centralized system and consequently has meetings with different departments and agencies on a regular basis. Even constitutional agencies that operate independently of the county need to be kept informed of and abide by IT policies and procedures. County-wide messaging regarding malicious activity is sent out as needed to employees 24 hours a day, 7 days a week.

Policy Development

Cybersecurity is not about any single challenge or department effort. Rather, the cybersecurity plan discusses how the county should approach the following enterprise-wide issues:

- Privacy and data security
- Scams and fraudulent activity
- Network security
- Website security
- E-mail security
- Mobile devices
- Employee education
- Facilities security
- Operations security and online payments
- Incident response
- Community Emergency Response Team (CERT).

The cybersecurity team meets with and obtains feedback from departments/agencies on a routine basis. Not all departments are open to talking, but before any policy or procedure or anything related to cybersecurity or technology is rolled out, the security team seeks departmental/agency input. "It's not just about us, but we have to understand how they do their job. We have to understand their business processes. We have to learn how they work and what their intent is in order to make the technology work for them and insure the technology is safe," said Vernon Greene, chief information security officer (CISO). "The security plan does this through improving processes and minimizing risks, and that is supported by quarterly audits." Examples of plan tactics include training employees about safe use of e-mail, like changing passwords frequently and using complex codes; encrypting data files before transferring onto the network; installing mobile security software on smartphones and tablets; and backing up network data on a routine basis.

The county's security plan is addressed no less than annually, but usually twice a year. Periodic reviews are undertaken as needed. The team intends for the plan to be a living document to guide the county's approach to cybersecurity. The plan is also presented to the Board of Commissioners for its education and understanding of the issues at hand. "Most of what we do is like having a large insurance policy. You don't want to ever have to use it, but it's critical to have it available in the event the worst happens," said Matelski.

Funding

It can be difficult to secure funding for security projects until something goes wrong and there is a financial or legal impact on the organization. When that happens, then people are willing to come to the table and talk about what can be done. However, the more that can be done in advance of an attack, the less actual damage will occur. "You don't leave your front door wide open, or if you lose your keys, I'm pretty sure you're going to change your locks," said Matelski. "We need to adhere to these same security practices at the computer and network levels."

Responding to Cyber Attacks

The IT and cybersecurity teams work hand in glove with the DeKalb Emergency Management Agency (DEMA). DEMA has responsibility for insuring continuity of operations (also known as COOP) in the event of an emergency. Many of the departments and agencies involved in IT and security planning are also involved in COOP planning. As a result, in addition to working through the annual IT and security planning process, a second annual review led by DEMA for COOP planning purposes is built in.

If the county experiences a malicious attack or other incident, the security team's plan calls for quickly bringing a small group together. DeKalb County has generally found that involving too many people in the response process is less effective, so the Community Emergency Response Team (CERT) does not involve all thirty departments. Instead, CERT focuses on quickly convening subject matter experts from key departments to form contingency plans. The size of CERT shrinks or grows depending on the issue to be addressed. To date, the maximum size of the team has been twelve people. In bringing together this small but knowledgeable group of experts, the intent is to respond and begin mitigation of incidents within the first thirty minutes of their occurrence rather than waiting twenty-four to forty-eight hours for all departments to meet. The team's goal is to plan and deploy a response within two hours of learning of a cyberattack.

The small team is generally comprised of representatives from the police department, other public safety agencies, and district attorney and IT staffs. These departments typically have access to security information before other departments. The county's commitment to being proactive and taking steps before an emergency occurs has resulted in not needing to call the group together for the past five years.

Collaboration

Most of the county's response to cyberattacks occurs in-house. The security team does, however, reach out and coordinate with other resources, including hardware and software vendors. They also rely on support from the National Institute of Standards and Technology (NIST), the Multi-State Information Sharing & Analysis Center (MS-ISAC), the *Financial Services—*Information *Sharing* and Analysis *Center* (FS-ISAC), the FBI, and other similar agencies. They also participate in several security user groups. The networks that the security team has established insure that they are not recreating the wheel in developing a response. The relationships also help identify leading practices and lessons learned.

One of the benefits of working on security issues in the public sector is that there's not competition between agencies or between different jurisdictions. In the private sector, two competitors are less likely collaborate or share information on their respective remediation plans. A company like Coca-Cola would not have an incentive to share information with Pepsi because of their competitive positions. Such a conundrum would not be an issue for the county, which often reaches out to have frank discussions with other local governments.

Staff Training and Communication

The plan points out that at some point during their tenure, nearly all DeKalb County employees will work on a computer. "We want to make sure every employee, no matter what job classification they hold, understands what the policies and procedures are and what acceptable computer use is," said Matelski. "We work at keeping people up to date on the latest threats. In addition to brown bag lunches, the team holds monthly and quarterly meetings with our Information Technology Advisory Council, which is comprised of technical and leadership staff from all county departments for sharing critical information." It's a very broad-based plan that incorporates various mechanisms for educating employees.

Matelski and Greene noted that in the cybersecurity field, and more generally in larger organizations, the weakest link is the individual end user. If any individual fails to follow prescribed policies or procedures, he or she can put the whole system at risk of being taken down. People often show little common sense or simply don't stop to think about what they are doing. It's also a function of social engineering attacks. Organizations can spend $100,000 or more for a new firewall or endpoint security, but it only takes one less-than-smart action by an individual to undo all that security.

DeKalb County has opted not to use consultants for much of its cybersecurity work. Team members have a long history of working in the field and have taken advantage of professional memberships and peer-to-peer connections to leverage the knowledge they need. The one exception to this rule is the county's annual subscription with the Gartner Group. The Gartner Group conducts technology research for global technology leaders. Professionals from Gartner visit the county once a year to assess and compare its work to other similar local governments. The group looks at everything the county does, not just cybersecurity concerns, and then presents their observations and comparisons.

The personal practices of staff have such an important role to play in safeguarding the county's computers and networks, so training for staff is imperative. Cybersecurity is one of the areas highlighted during onboard training for new employees. The six-hour training for new employees includes twenty minutes devoted to cybersecurity governing policies and procedures. Acceptable uses of county hardware and software systems, mobile applications, and data security are specifically on the agenda.

> ***"Even with all the knowledge and resources available, people continue to be tricked or duped into doing things that simply don't make sense," said Greene. "We've seen notifications about viruses go out through the news and mass media warning of a security threat. Curiosity still gets the better of people and they click the link."***

Other means for communicating with staff about changes in security processes and procedures include: notices being sent out as needed 24/7, formal training offered to personnel, informal brown bag lunches, posting resource materials on the intranet site, and a quarterly newsletter that is sent out electronically and made available through the website. Computer-based training (CBT) is made available for staff to take any time. IT personnel also may be contacted via phone or e-mail to address emergency issues that may pop up outside of traditional business hours. For example, if an employee receives a suspect e-mail attachment, it can be sent to the IT department for evaluation at any time.

Monitoring

With so many assaults and attacks coming from outside the organization, it's imperative for IT personnel to be addressing the different types of attacks taking place and those emerging. It's about protecting the perimeter of the organization. Unfortunately, it's not just attacks coming from outside the organization, but inside as well. These internal attacks can be equally crippling to the organization, so monitoring what is happening within the system is critical. Tactics for monitoring internal attacks include the following:

1. Conduct annual enterprise-wide risk assessments—Organizations must take an enterprise-wide view of information security, first determining its critical assets, then defining a risk management strategy to protect those assets.
2. Enforce separation of duties—Effective separation of duties requires the implementation of what is called "least privilege," authorizing people only for the resources they need to do their jobs.
3. Log, monitor, and audit employee online actions—Logging, periodic monitoring, and auditing provide an organization the opportunity to discover and investigate suspicious insider actions before something serious occurs.
4. Deactivate computer access prior to or immediately following termination—When an employee is terminated, regardless of reason, it is important that the organization have in place termination procedures that disable all of the employee's access points to the organization's physical locations, networks, systems, applications, and data.
5. Collect and save data for use in investigations—Should an insider attack, it is important that the organization have evidence in hand to identify the insider and follow up appropriately.
6. Clearly document insider threat controls—As an organization acts to prevent insider threats, clear documentation and procedures will help ensure better protection and better understanding by employees, as well as eliminate misconceptions that anyone is being targeted in a discriminatory manner.

Recovery

DeKalb County has had no significant breach to its system over the last five years (2012–2017). There was one smaller breach that attached itself to three PCs in the Board Commissioners offices, a department that gets inundated by e-mail. The issue was identified within sixty seconds, and staff shut down the network ports of the infected devices immediately. The delivery mechanism was an e-mail that appeared to be from a reputable source, but proved to be a ransomware application that was downloaded from an external file hosting service.

The county's intrusion prevention system (IPS) captured and prevented the worm from going any further than those three devices. Three people from the IT security team confiscated the PCs and cleaned the hard drives. The cost of addressing this incident included five to nine hours of work with minimal cost, perhaps $150 to $200 of staff time. Greene noted that had the worm not been discovered so quickly, the damage could have run in the hundreds of thousands of dollars. As it was, the security team was able to completely restore all data to the computers and had no data loss.

With respect to ransomware, Matelski commented that most organizations do a good job of backing up their data onto a network server, but a poor job of backing up hard drives by relying on the end user (i.e., the employee) to back up data and programs from the C drive of individual PCs. In fact, DeKalb County doesn't back up local hard drives and makes a point of conveying to departments and staff that they don't. If a ransomware attack were to occur, it would be difficult, if not impossible, to restore the data on the C drives. For this reason, employees are encouraged to save data to network drives. In general, it's challenging to educate staff and make sure people are following policies, procedures, and common sense.

Lessons Learned

- **Cybersecurity is an enterprise-wide concern**. Executive leadership is required, not just an IT response to the challenges that spring up. Planning and following security policies and procedure need to be part of the organizational culture. Local government staff need to understand cybersecurity is both a top-down and bottom-up concern for everyone working with a local government computer.
- **Ransomware and other cyber threats are not going away.** The number of cyber attacks will continue to increase as will the creativity of those threats as long as people are paying the ransom.
- Technology solutions can catch a large portion of the threats, but viruses can morph in a very short time period. **Machines cannot catch everything**.
- **Perimeter network security is very important, but end-point security trumps that, and common sense is the most important element in developing a strong cybersecurity plan.** Local governments need to take a three-pronged approach—perimeter network security, end-point security, and common sense—in shoring up their perimeters, including doing all they can to educate people on security matters.
- With the increasing number of cloud solutions, **integrations and integration security are essential**. While cloud and software as a service (SaaS) vendors provide security as part of their service and will have service level agreements as part of the contract, the local government still owns the data. If something happens to the solution or data is lost or destroyed, the responsibility for restoring operations remains with the local government.
- **Threats from insiders remain a significant challenge**. Individuals on their way out of an organization pose a potential threat to data security and system-wide performance.

> ***"We are all still vulnerable to the simplest of attacks. The insider threat continues to be a major concern for businesses of all sizes," said Matelski.***

- **The Internet of Things (IOT) is here**. There are many devices—water meters, parking meters, traffic sensors—that generate a tremendous amount of data that must be protected. It becomes difficult to secure these data as more such devices become available for service delivery. Special attention must be given to develop appropriate strategies for securing the new data, and good relationships with vendors must be maintained.
- Most IT departments employ highly technical staff with critical skill sets, **but it is possible to become too technical,** especially when working with a large number of employees who have varying skill levels. At the most fundamental level, it's important that staff understand the need for strong cybersecurity measures and the potential dangers of not following policies and procedures.
- **IT departments should request funding for personnel and other resources**, but many times those requests don't get approved because it is seen as an expensive insurance policy. The challenge is to demonstrate that it's less expensive to be proactive in protecting critical infrastructure than to repair or replace systems or data that are lost by cyberattacks.

Study Interviewees

John Matelski, Chief Innovation and Information Officer (CIIO) and Director of Innovation and Technology (IT), DeKalb County, Georgia

Vernon Greene, Chief Information Security Officer (CISO), DeKalb County, Georgia

Jefferson County, Alabama—Community Profile

- **Population:** 660,367 (2016)
- **Median Household Income:** $45,239
- **Cybersecurity Budget**: $350,000 annually
- **FTEs Working in Cybersecurity**: ¾ of 1 FTE

Background

Security and cybersecurity have always been concerns for Jefferson County, Alabama. The county operates a medical facility that is covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regulations. Compliance with HIPPA regulations requires that the county must protect patient privacy. Consequently, ever since the medical facility's first computer system was installed, a firewall has existed.

While security has always been a concern for the county, the increased threat to cybersecurity that began a few years ago requires the county to be prepared to fight cyber attacks on a continuous basis. The county's IT team developed a formal plan with appropriate strategies to protect the county's computer systems. The county's IT team looks at the issues of security and cybersecurity as two parts of the same question: security is just part of the everyday business of IT whereas cybersecurity requires everyone to be aware and be at the ready for attempts outside the organization to hack into systems.

Jefferson County continually looks at what technology solutions are available. The county uses information from Gartner, an information technology research and advisory company, to determine what the best technology solutions are. The research firm has labs for conducting testing that most local governments cannot afford to do for themselves. IT team member Allen Franklin, Jefferson County's network systems administrator, referred to Gartner as a *Consumer Reports* for technology companies and departments. The IT department relies on Gartner to do the heavy lifting and to research the relative positions of available technology solutions. For example, the IT department might use Gartner to determine which anti-virus software has proven to stop the most malware. The county looks at solutions listed in the "Gartner Magic Quadrant" and works to implement products that represent the best of class.

A Plan for Security and Cybersecurity

To develop a formal plan for security and cybersecurity, the IT team secured the services of an outside firm, Dynetics, to do a needs analysis and conduct penetration testing. Penetration testing is used to check computer systems, networks, and web applications to discover possible vulnerabilities that an attacker could exploit.

The consultant also conducted internal and external evaluations of the threats to the county's systems, looking at IP addresses, internal servers, websites, web environment, and other related systems. The consultants identified areas within the computer systems that were considered critical and designated them as high priorities for additional study and work. For example, the consultant identified the assignment and maintenance of email addresses as a concern. The county needs to know which active email accounts are valid and being used properly. Other concerns included the need for employees to use encryption when sending personal information and to have an awareness of how to identify and avoid phishing emails. The county has maintained a working relationship with the consultant, who has a two-year renewable contract.

Following the penetration testing, a team including Roosevelt Butler, interim chief information officer, and Douglas Taylor, senior systems architect, drew up a plan that the IT team adheres to in its daily operations. The county updates its security and cybersecurity plan once a year. Elements of the plan include the following components:

Ransomware. One of the key chapters in the plan addresses the county's need to protect against ransomware. In 2016, the county was subject to five ransomware attacks over an eight- to nine-month time period. The series of attacks forced the county to take a step back, assess its current environment, and devise a new strategy. The county ended up enhancing and overhauling its desktop security strategy, thereby deploying a new desktop security software framework to readily protect endpoints from malicious activity.

Web security. The IT team has studied web security very closely. After ransomware attacks, the county installed a new network appliance/device, Deep Discovery Inspector, which it uses to monitor network traffic and detect and protect against targeted attacks within the network. The IT team has also brought in a web security program, Blue Coat, designed to control, monitor, and secure Internet use by employees. The program prevents a small number of users from hogging bandwidth, exposing the network to malicious software, or leaking internal documents.

The program started as an on-premise solution, though the county subsequently decided to move it to the cloud. This decision was made to gain a higher level of security through cloud-based technology. The new technology uses a vast array of data scans from a large number of clients. As a result, the service offers a near real-time identification of threats, blocking of threats, and preventive solutions. With a cloud solution, there is no hardware or software to deploy, update, or manage. The county does not have the issue of end-of-life (EOL) equipment or EOL solutions. Scheduled downtime due to updates or upgrades is a practice of the past. The county also realized a substantial cost savings by moving to the cloud.

Web traffic. The county monitors web traffic for security threats using a sandbox. *A sandbox* is a security mechanism for separating running programs. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users, or websites, without risking harm to the host machine or operating system.

Email. The county has multiple levels of security for email. The county uses an on-premise appliance, CISCO IronPort, for the first line of defense for the following services: anti-spam protection, spam management, and anti-malware protection. Microsoft Office 365 Exchange Online Protection serves as secondary defensive posture for email services.

Structure of IT

The IT team operates as a centralized service and is responsible for addressing all security and cybersecurity needs for the county. As such, the team determines the strategies to adopt, buys the hardware and software, and puts them in place. Within the department, IT is organized by divisions, including one for desktop support, network, and server. Each division has responsibility for security and cybersecurity as it relates to their respective areas; for example, desktop support has responsibility for managing anti-virus security, and the network division has responsibility for maintaining the firewall.

Training and Education

The county oversees a budget for security and cybersecurity training with the IT team working together to determine what training would benefit the county most. Besides providing targeted one-off training opportunities, the team participates with training associations that provide ongoing training through newsletters, monthly tests, and other tools. The county hopes to develop internal and possibly external training classes to educate employees about cybersecurity threats and how to prevent future attacks.

Challenges

Securing funding for security and cybersecurity projects has not been a major issue for the county as is often the case with many local governments. The greater challenge for the IT department is staffing and maintaining dedicated staffing levels to work on any one project. “Staffing is a huge issue because you need someone to be primarily responsible for each project. With the lack of staff, we simply don’t have the resources to look at the systems the way we should on a daily basis,” said Butler.

Identifying serious security/cybersecurity events involves assessing the size and magnitude of an event. One of the prevalent fears among members of the IT team is the “click on link” scenario that spreads a virus and has the potential to shut down systems.

The loss of data through ransomware attacks was problematic because restoration took so much time. While the data were restored quickly, resetting all of the security settings was very time-consuming. The attacks in 2016 took considerable time to resolve, but they are not the only cybersecurity issues the county has faced.

Prior to the attacks, the county’s mainframe at the Sheriff’s Office was hacked and private personal data were released on the web. The FBI got involved with the case, which was determined to be the work of a member of Hackers Anonymous. The FBI caught the individual responsible for the hack, but there was no recovering from the release of private data, which affected many individuals.

“When a security/cybersecurity event does occur, it is important to triage the event and determine if it has spread throughout the global enterprise. If you have an event and it involves a single person’s machine, that’s one thing. But if it has spread through several departments, it’s problematic. We have to be prepared to quickly make that assessment,” said Butler. During the recovery period, Butler also emphasized the need for very clean data. Data needs to be quarantined and thoroughly cleaned before being restored to ensure that the same thing doesn't happen again.

Since the ransomware attacks, the county has changed its desktop software and has been fortunate to not have had another successful attack. The county did not track the exact number of labor hours spent on recovery, but estimates it spent $75,000 to $80,000 in purchasing new anti-virus software and updating other software applications.

Lessons Learned

- **Penetration testing** is eye-opening and helps government leaders understand how many attacks are made day in and day out.
- Among the most important practices the county shared is the need to **have good data backups**. IT team members advised that local governments always maintain at least three months' worth of data and closer to twelve months if space permits.
- **Monthly security and critical patches** should be installed on all desktops and servers.
- Local government IT staff should be diligent about **staying current with the newest security/cyber-security technology and install the right software and hardware where it's needed**.
- Lastly, the Jefferson County IT team members emphasized that **local governments shouldn't shortchange the security budget**. The budget should be based on a needs assessment, accompanied by solid research and knowledge on what new threats are out there. Local governments should use that information to determine what tools to have in place.
- **The costs of a few prevention measures are minimal compared to the costs if the organization is not prepared for an attack.**

The team said IT staff should always work to make the organization more secure than it is now. Success for Jefferson County is measurable: it has gone from five attacks in less than a year to no successful attacks as of yet in 2017.

Study Interviewees

Roosevelt Butler, Interim Chief Information Officer, Jefferson County, Alabama

Chris Bookout, Database Administrator, Jefferson County, Alabama

Keith Gulledge, Network Systems Administrator II, Jefferson County, Alabama

Joe White, Technical Infrastructure Manager, Jefferson County, Alabama

Willie Wright, Senior System Analyst, Jefferson County, Alabama

Allen Franklin, Network Systems Administrator II, Jefferson County Commission

Douglas Taylor, Senior Systems Architect, Jefferson County, Alabama

City of Roseville, California—Community Profile

- **Population:** 135,868 (2017)
- **Median Household Income:** $80,658
- **Cybersecurity Budget:** approximately $400,000 annually
- **FTEs Working in Cybersecurity:** 1.0 FTE (Information security administrator). NOTE: The city uses a cross-functional approach and work team from the human resources, police, utilities, and information technology departments for a total of 11 team members.

Background

Questions regarding the security of the city of Roseville's computer systems were first brought up at city council meetings in 2017. In many communities, high-profile city services such as transportation, public safety, and communications tend to receive the most interest from council members, while back-end services like human resources and finance are treated as second-tier programs. Roseville's city council does not think this way; they understand that back-end programs are equally important. "We have done a really good job of communicating with the council about how IT supports the overall efficiency and business life of the city. We have kept reminding them that the Internet touches nearly every aspect of daily life now," said Hong Sae, chief information officer, City of Roseville, California.

Roseville is a full-service city located in the Sacramento Metropolitan Area, and its agencies/departments provide water, power, police and fire, parks, recreation, library, economic development, and public works/development services, as well as many other administrative services to its nearly 136,000 residents. Early on, many council members didn't understand the full extent of reporting requirements, as required by regulatory agencies, organizations, and legislation, including those listed below::

- U.S. National Institute of Standards and Technology (NIST)
- Payment Card Industry Data Security Standard (PCI)
- North American Electric Reliability Corporation (*NERC*)
- Federal Energy Regulatory Commission (FERC)
- U.S. Department of Homeland Security (DHS)
- Criminal Justice Information Services (CJIS)
- U.S. Food and Drug Administration (FDA)
- U.S. Federal Emergency Management Agency (FEMA)
- Sarbanes-Oxley Act (SOX)
- Health Insurance Portability and Accountability Act (HIPPA)

The formal relationship with these agencies dictates that the city must be in compliance with the security requirements of each agency.

Building a Culture: Security Is Everyone's Business

Cybersecurity came to the forefront of the council's agenda because it is so critical in the work of the city. The city doesn't maintain one central plan for security and cybersecurity, but rather views the responsibility for maintaining a secure environment as belonging to all departments. The city has adopted an approach to security and cybersecurity in much the same way as the Transportation Safety Administration (TSA) has used the brand, "Security Is Our Business." All employees are expected to follow security and cybersecurity practices in their daily operations.

The city has developed many policies designed to strengthen and preserve the integrity of its computer networks. To date, policies have been developed for networking, identity theft protection, and incident response. These policies have benefited not only the city but also other local governments in the state. The California legislature has enacted many measures for identity theft protection and emergency management notification. Roseville has advocated for many of these changes at the state level. The city has also actively participated in the development of cybersecurity policies for local governments, including a cyber emergency annex policy that was created and formed by FEMA.

Simply having policies on paper isn't enough, though. Roseville has made a practice of testing its policies on a routine basis. In the space of three years, the city has run three emergency desktop exercises based on its policies to test computer systems and see how well the city responds when faced with a breach, attack, or other incident. The city participated in the Northern California Cyber Desktop event in San Francisco in 2015. It carried out the first Northern California Local Government Emergency Operations exercise in Roseville. The city also attends the quarterly FEMA emergency cyber events, which present scenarios requiring a quick response. The exercises are all about practice. “Practice makes perfect,” said Sae.

Analysis of the exercise results has been instructive for government leaders. Whether the exercise is focused on electrical grid failure or a hacker infiltrating the city’s electronic fund transfer application, one consistent result is the need to anticipate the unknown and be prepared to respond to change, moment to moment. The Petya ransomware that hit Europe in June 2017 is one example, with the Multi-State Information Sharing & Analysis Center (MS-ISAC) issuing a warning regarding the virus, including notes on its symptoms.

The Roseville IT team is proactive in preparing for its incident response, focusing on not only the technology but also the people and processes. Technology comes first, and the team makes sure the city has the latest anti-virus and malware prevention programs and other solutions. The team recognizes it is also important to have policies and processes in place that reflect city priorities should an attack occur and to have people trained to manage the city’s response.

IT is the lead department in planning for information security and cybersecurity, but the department works very closely with the city’s HR and risk management teams in determining an appropriate level of cyber liability insurance to cover the city’s needs should its network go down due to an attack. About seven years ago, the city was hit with a zero-day malware, which means there were no fixes or patches available. The response took an all-hands-on-deck approach as the virus brought the city’s network to a crawl. Ultimately, the breach was contained quickly and personal identification data were protected. But for a time, the city had no revenue streams coming in or going out, and many staff members were unable to work. As a result of these unforeseen expenses, the city started purchasing cyber liability insurance in 2015 as an extra safety measure in the event of a future incident. The liability insurance takes the city to the next level in its cybersecurity maturity. Still, one of the most difficult challenges is to drill down to that first individual and that first computer to determine where a breach took place on the network.

In addition to working with the HR and risk management teams, IT collaborates with the utility groups on providing awareness training for payment card users; the fire department, which helps plan incident response processes; and the communications department, which works on remediation processing and communicating with the council and the public. “A lot of local governments work in silo environments with their IT department being solely responsible for information security and cybersecurity, but we believe plans need to be owned and implemented by all departments,” said Sae. The council and the city manager have been very supportive of the IT department’s approach to cybersecurity, and the IT department makes sure to notify all city leaders when there is a breach or other incident.

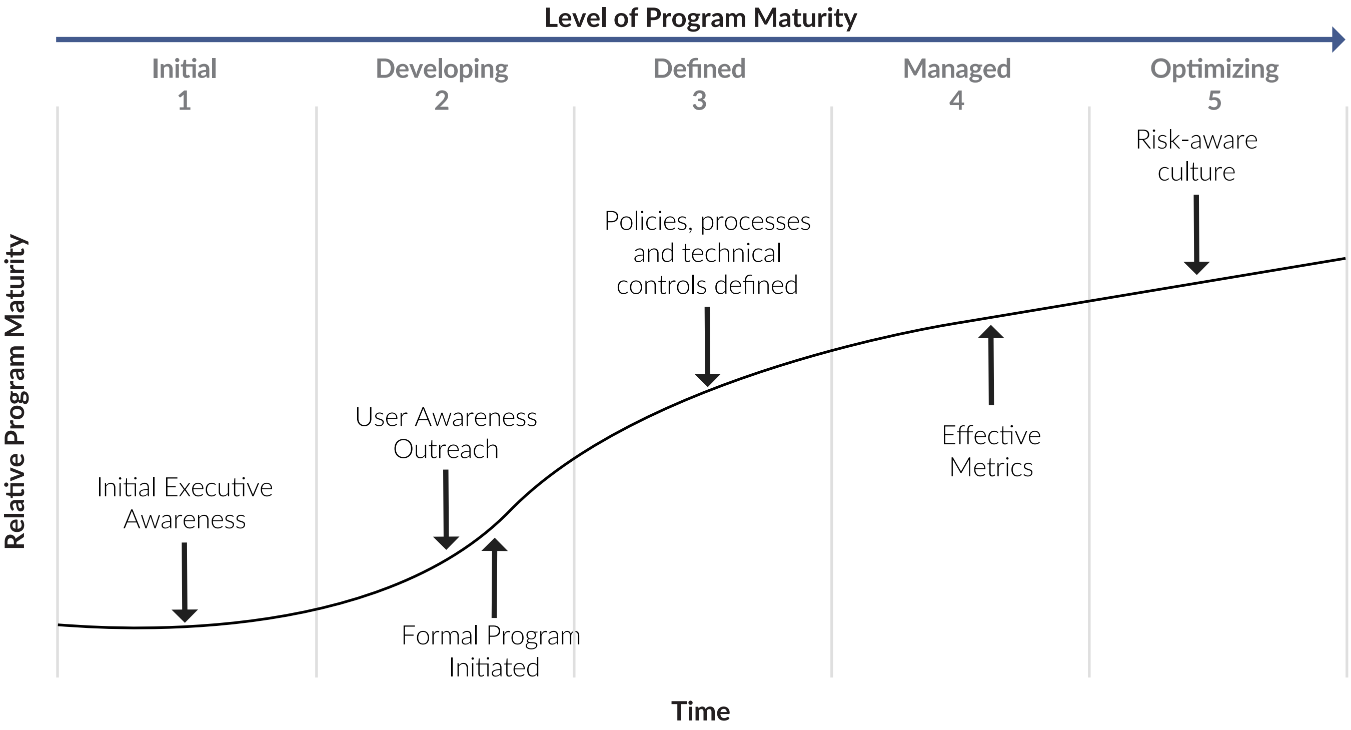
External Resources

The IT team relies on its vendors for assistance on their response plans. The city of Roseville might have one or two attacks a day, whereas vendors will have to contend with hundreds of attacks every day. Their experiences are invaluable in dealing with a response process. The city has two vendors with which they have had long-term business relationships: Moss Adams, which provides information technology strategic planning services, and Optiv, which is a vendor-neutral cybersecurity organization that designs cybersecurity solutions using industry best practices with clients.

The city has mandated that policies and plans should be updated every two years, but events on the world stage force changes to take place faster than that. Security work is more continual and needs to be updated daily. One IT staff member researches best practices routinely and updates the city’s policies based on developments as they occur. “It’s just part of good project management,” said Sae. For example, the city may have a requirement that penetration and vulnerability testing be conducted every quarter, but if the payment card industry is dictating a change in its best practices, the city would be hopelessly behind if it stayed with the original two-year plan.

The city uses consultants in its security and cybersecurity efforts and looks to work with those who have advanced credentials, given the city’s maturity level in cybersecurity (see the “Cybersecurity Program Maturity” graphic). When seeking a consultant, the city

Cybersecurity Program Maturity



Source: Optiv

sends out a request for proposals (RFP) that defines the city's requirements, including the need for certification, advanced training, day-to-day engagement, and other efforts undertaken to keep up-to-date on incidents happening in the field. In reviewing proposals, it's critical that the right products and services be purchased for the city.

Moss Adams works with the city on the development of its strategic technology plan and conducts an annual check-up to ensure that the city's annual plan and its strategic technology plan line up. The relationship with Optiv focuses on bringing the city to the next level of security maturity. Consultants advise city leaders about best practices emerging in the field and what the city needs to do to improve its maturity level. Maintaining the infrastructure base helps the city conduct risk assessments and ensures the city gets the biggest bang for its buck.

On the public sector side, the city has worked with the FBI on system attacks as well as MS-ISAC to respond to new attacks. MS-ISAC works to improve the overall cybersecurity environment of the nation's state, local, tribal, and territorial governments through focused cyber threat prevention, protection, response, and recovery.

Training and Education

The city is active in several peer knowledge-sharing groups such as Municipal Information Systems Association of California (MISAC), IT-Security: Federal Listserv, and MS-ISAC. When a widespread attack does occur, members of these peer groups share information with each other through a mass distribution list. Such networks serve as a critical source of information in developing ideas on how to respond to and contain new attacks.

IT staff have been encouraged to participate in key industry events such as Black Hat Briefings, a computer security conference that provides security consulting, training, and briefings to ethical hackers, corporations, and government agencies. The WhiteHat Security conference focuses on application security, enabling businesses to better protect critical data, ensure compliance, and manage risk. Conferences such as these provide a wealth of "just-in-time" information.

In 2016, the city moved to more online training, but it has also hired a chief information security officer/information security administrator (CISO/ISA) who works closely with the HR department to provide internal security training for staff members. The city requires respective individual IT staff members to maintain certification such as a certified information systems security professional (CISSP) or a certified ethical hacker (CEH).

The city makes a point to provide advanced-level training to staff. Training on the use of an application alone is not sufficient. Staff are also trained on how to create policies and procedures. IT staff are expected to know how to work with people and balance competing needs during a security/cybersecurity event. "Security is all about providing the right level of access to users so that citizens can be comfortable that their private utility information won't be shared with the wrong person. The city manager and the council also need to have confidence that the city has safeguards in place to prevent any personally identifiable information (PII), which could potentially identify a specific individual, from getting into the wrong hands," said Sae.

Sae notes that people are the most difficult part of managing security and cybersecurity initiatives. People generally don't anticipate the need for change, and many are unwilling to change. At times, the IT staff may find it difficult to explain why a procedure that seems to be working well for the organization today needs to be changed three months down the road. The central message that needs to go out to staff is that technology is ever-changing and no system is completely secure. People need to understand their role in keeping systems safe.

Communication

Communication is key. All city leaders and staff need to be kept informed and know what the city's response is during a cyber attack. It's akin to how FEMA would respond to a flood or other emergency. Things move fast during an event, and the city must use multiple communication channels to keep everyone informed of actions being taken. The recent WannaCry and the Petya ransomware attacks are two examples of how quickly attacks can spread in the global community.

After a cyber incident, city staff take time out to prepare reports that can be very helpful in identifying how to improve the city's response in the future. There are numerous viruses and other malicious software to stop out there. It is important to take the opportunity to communicate to the city council, the city manager, and the public about what transpired and how the city responded. IT staff make a point of reporting information to the public when incidents occur. "Taxpayers need to see their dollars at work," said Sae.

Lessons Learned

Perfect security and protection don't exist. Local governments must engage in a constant balancing act between data privacy and system availability. Managers need to focus on improving their processes to reach new maturity levels. U.S. communities and businesses have achieved a good degree of security in this new world order, but in this global economy, IT managers must be aware that breaches that occur in less mature environments can still spread quickly.

All local governments have a role to play in protecting the U.S. infrastructure from cyber attacks. Local government officials should not be afraid to share information and experiences with their peers. There is a lot to learn and everyone benefits from increased communication. And while the public tends to assume that all data maintained by state and local governments is available for public consumption, some data are personal or sensitive in nature and not subject to open-record requests. It's critical to know what hackers are thinking about and where they get their information.

Study Interviewee

Hong Sae, Chief Information Officer, City of Roseville, California

About the Authors

Cory Fleming, a senior technical specialist with ICMA, has written about the use of data for improved local government service delivery and performance measurement in various capacities. She currently directs the #LocalGov Technology Alliance, an initiative started with Esri, the premiere geographic information system (GIS) software solution, to explore the world of big data, open data, apps, and dashboards, and what it all means for local governments. She served as the editor of *The GIS Guide for Local Government Officials*, a joint publication produced by Esri and ICMA and released in 2005. A subsequent joint publication, *The GIS Guide for Elected Officials*, was released by Esri Press in January 2014.

Will Fricke is an ICMA intern, working primarily with the Research and Policy team. Will graduated from the University of Connecticut in 2017 with a bachelor's degree in political science and economics.

Roger L. Kemp is a career city manager, having worked in and managed the largest cities with the council-manager form of government in the states of California (Oakland), New Jersey (Clifton), and Connecticut (Meriden). He also taught graduate courses during his city management career, and presently holds the titles of professional in residence in the Department of Public Management at the University of New Haven and distinguished adjunct professor in the executive MPA program at Golden Gate University. Roger is also a life member, legacy leader, and mentor in the International City/County Management Association (ICMA). He received his MPA from San Diego State University; his MBA from Golden Gate University; and his PhD from Golden Gate University.

Laura Mateczun is a graduate of the University of Maryland Francis King Carey School of Law and a member of the Maryland Bar. She is currently a PhD student at the School of Public Policy at the University of Maryland, Baltimore County, as well as a research assistant for the Maryland Institute for Policy Analysis and Research. Her policy interests are interdisciplinary in nature and span fields from criminal justice and local government cybersecurity to health care and public management, focusing on issues of equity and efficiency.

Donald F. Norris is director of the School of Public Policy and director of the Maryland Institute for Policy Analysis and Research at the University of Maryland, Baltimore County. His fields of study include public management, in which he specializes in information technology in governmental organizations, including e-government and cybersecurity; and urban affairs broadly but with specific attention to metropolitan governance. He has published widely in leading journals in urban affairs and public administration. His latest book, *Metropolitan Governance in America*, was published by Ashgate Publishing in 2015. He received a BS in history from the University of Memphis and an MA and PhD in political science from the University of Virginia.

Appendix A-1: Summary Report of Survey Results

Introduction

In 2016, the International City/County Management Association (ICMA), in partnership with the University of Maryland, Baltimore County (UMBC), conducted a survey to better understand local government cybersecurity practices. The results of this survey provide insights into the cybersecurity issues faced by U.S. local governments, including what their capacities are, what kind of barriers they face, and what type of support they have to implement cybersecurity programs.

Cybersecurity 2016 Survey

	Number Surveyed	Number Responding	Response Rate
Total	3423	411	12.0%
Population Size			
Over 1,000,000	42	11	26.2%
500,000—1,000,000	98	20	20.4%
250,000—499,999	168	26	15.5%
100,000—249,999	532	63	11.8%
50,000—99,999	939	108	11.5%
25,000—49,999	1644	183	11.1%
Geographic Division			
New England	183	23	12.6%
Middle Atlantic	391	23	5.9%
East North Central	782	94	12.0%
West North Central	266	26	9.8%
South Atlantic	541	79	14.6%
East South Central	253	20	7.9%
West South Central	354	41	11.6%
Mountain	220	48	21.8%
Pacific Coast	433	57	13.2%
Type of Government			
Municipalities	1893	267	14.1%
Counties	1530	144	9.4%

Methodology

The survey was sent on paper via postal mail to the chief information officers of 3,423 U.S. local governments with populations of 25,000 or greater. An online submission option was also made available to survey recipients. Responses were received from 411 of the governments surveyed, yielding a response rate of 12 percent. Cities were overrepresented among respondents while counties were underrepresented. Similarly, there were a higher percentage of responses received from larger communities compared to smaller communities. Further, jurisdictions in the Mountain region of the United States were overrepresented, while jurisdictions in the Middle Atlantic and East South Central regions were underrepresented. The following report reflects trends among the unweighted survey responses, and should only be considered to be representative of the responding governments. Weighting should be applied to achieve representation of the broader survey population.

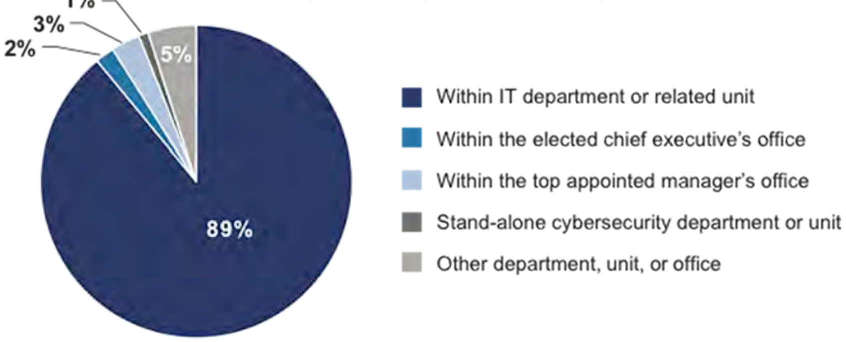
Survey Highlights

This survey provides insight into the cybersecurity practices among local governments in the United States. Key topics explored include which departments are responsible for cybersecurity; awareness of and support for cybersecurity; what barriers local governments face to achieve higher levels of cybersecurity; and what cybersecurity practices and tools local governments are using. Highlights from the data are outlined below, and responses to survey questions are summarized in the appendix.

Information Technology and Cybersecurity

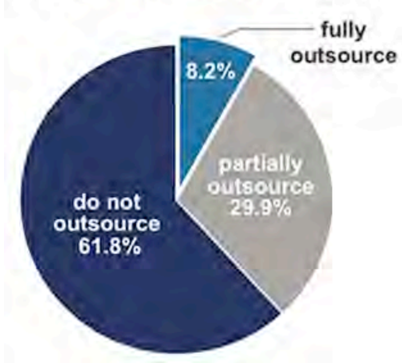
Primary responsibility for cybersecurity is located within the information technology (IT) departments in most of the responding local governments. Only 1 percent of the responding local governments have a stand-alone cybersecurity department or unit.

Where is the primary responsibility for cybersecurity located in your local government's organization?

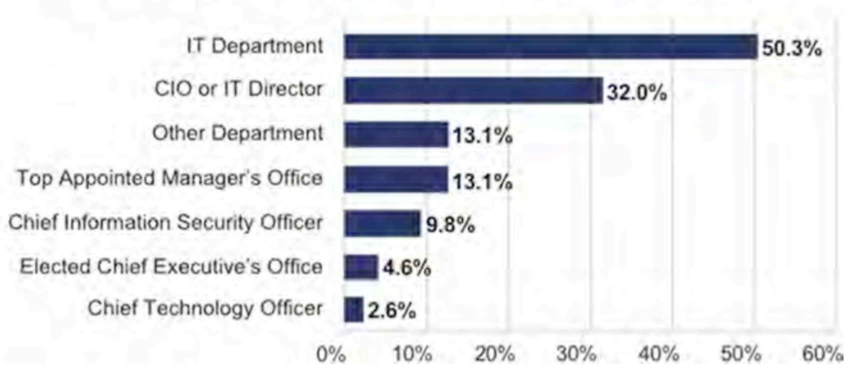


Most of the responding local governments do not outsource cybersecurity functions (61.8%). For the ones that outsource (38.1%), the contractors mostly report to the IT department (50.3%).

Does your local government outsource any of its cybersecurity functions?



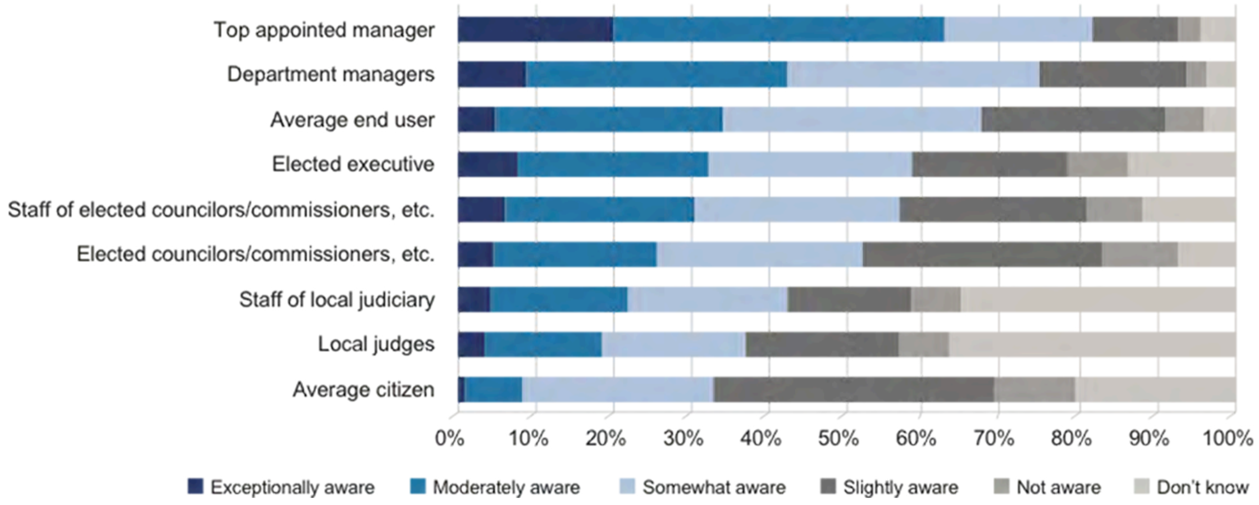
If outsourced, to what office or official in your local government does the contractor(s) to whom you outsource cybersecurity report?



Cybersecurity Awareness, Support

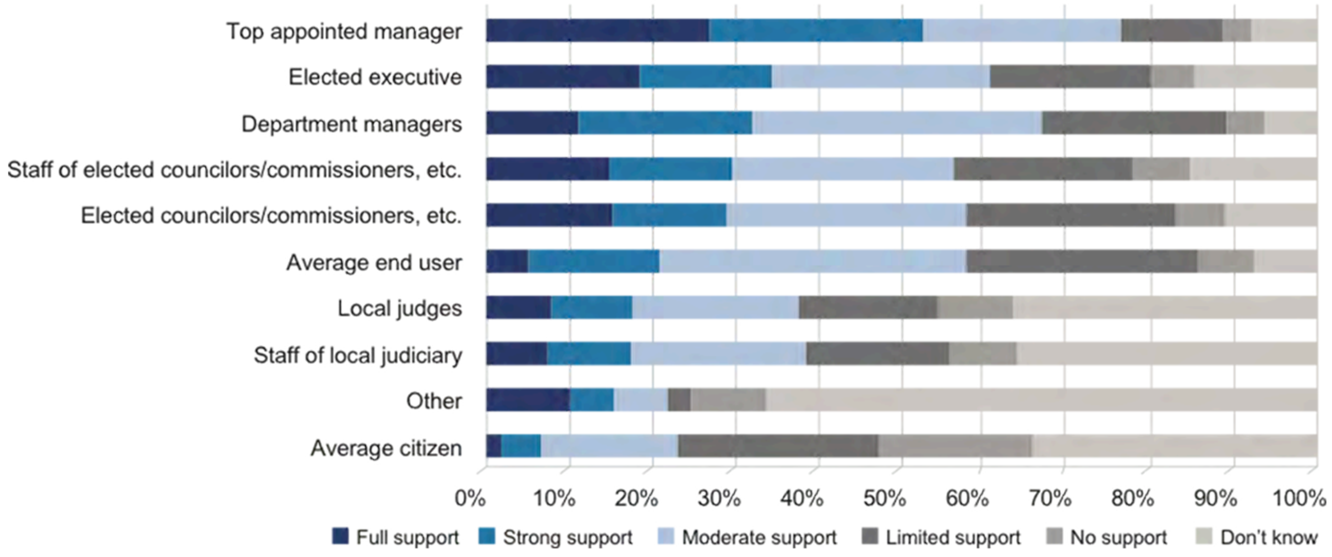
Among the responding local governments, a significant percentage of top appointed managers (61.7%) and department managers (42.5%) were either moderately or exceptionally aware of cybersecurity issues.

How would you rate the cybersecurity awareness of each of the following in your local government?



More than half of top appointed managers (53.8%) provide either strong or full support for cybersecurity, while one-third of the elected executives (35.6%) and department managers (33.3%) provide either strong or full support.

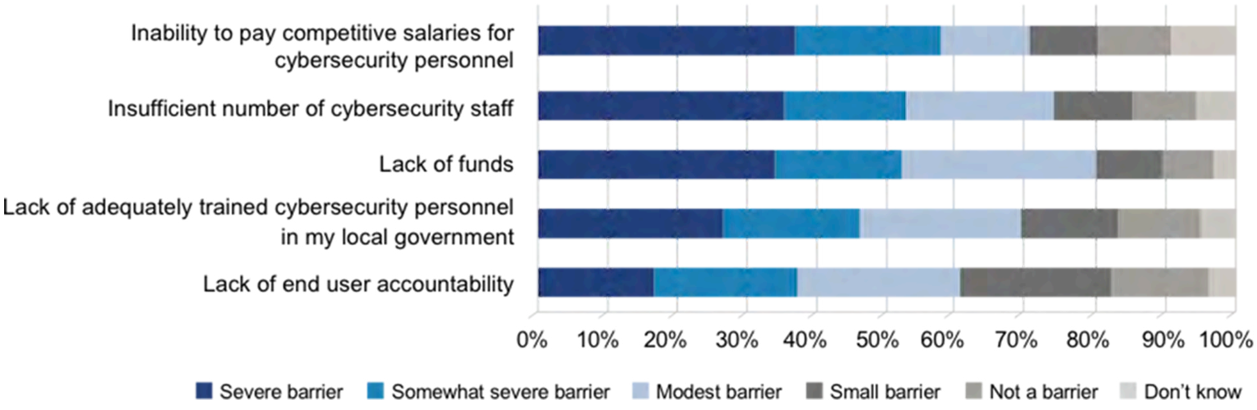
How would you rate the amount of support that cybersecurity receives in your local government from each of the following?



Barriers

Inability to pay competitive salaries for cybersecurity personnel (58.3%), an insufficient number of cybersecurity staff (53.0%), and lack of funds (52.3%) were identified by responding local governments as severe or somewhat severe barriers to achieving the highest possible level of cybersecurity.

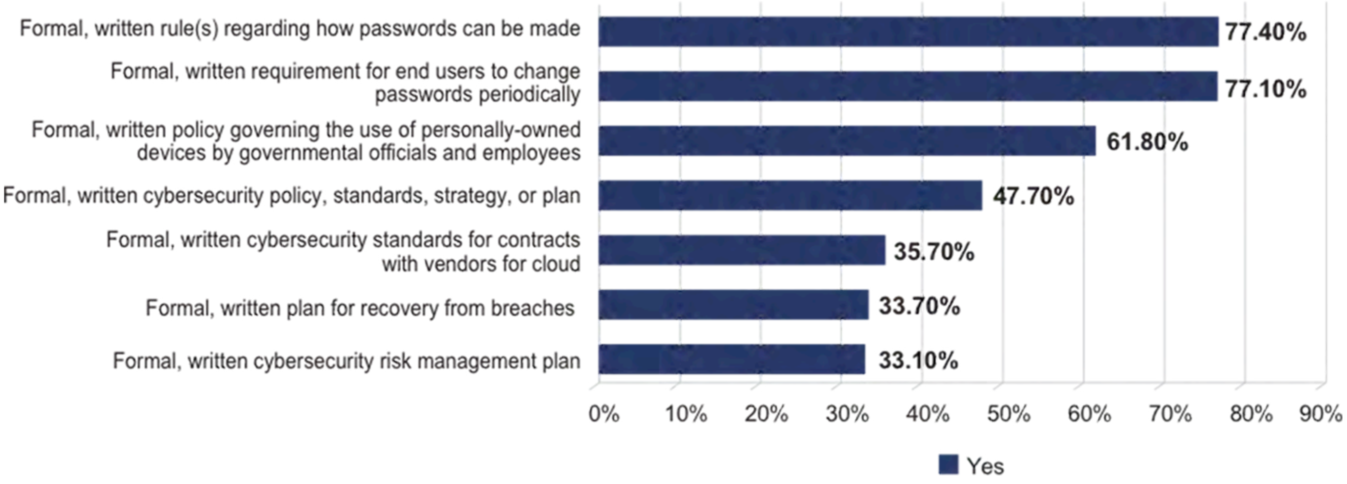
To what extent is each of the following a barrier for your local government to achieve the highest possible level of cybersecurity?



Cybersecurity Practices, Policies, and Tools

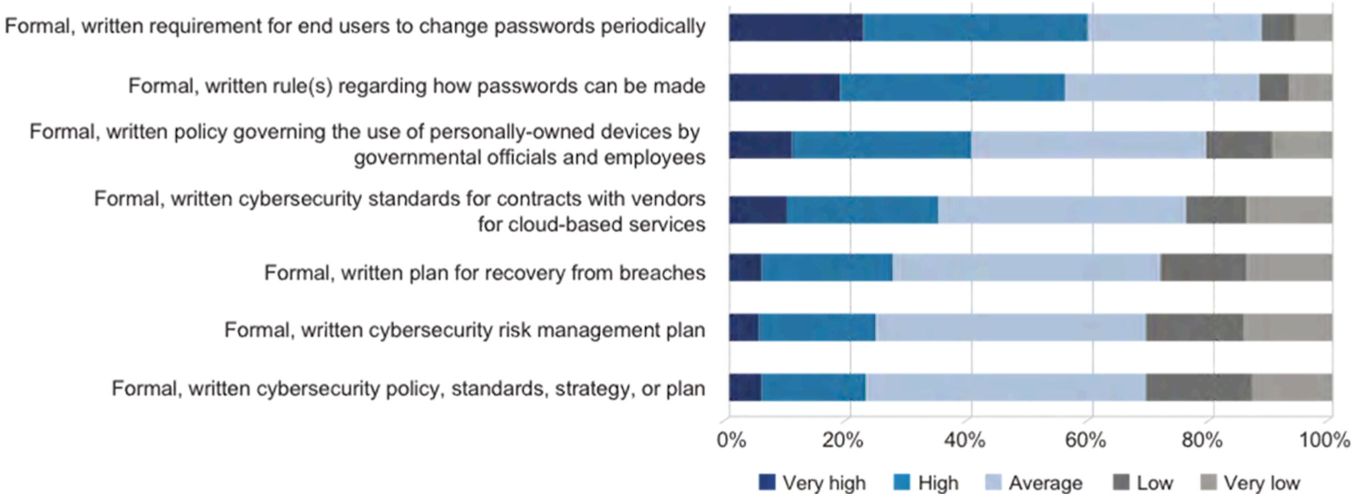
A significant proportion of responding local governments developed rule(s) regarding how passwords can be made (77.4%), a requirement for end users to change passwords periodically (77.1%), and a formal policy governing the use of personally owned devices by governmental officials and employees (61.8%).

Has your local government developed any of the following?



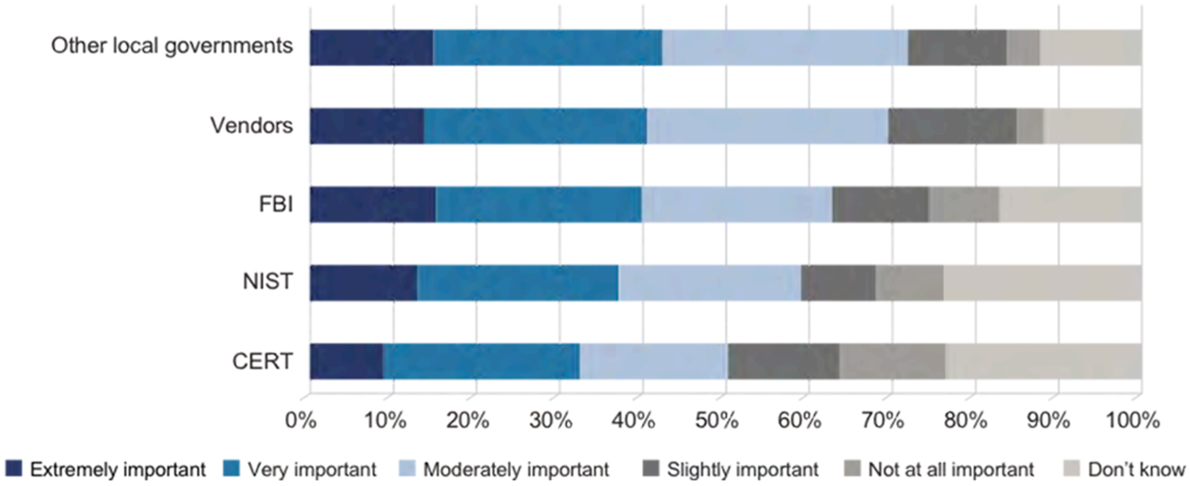
As a follow-up, respondents rated the following three cybersecurity measures as the most effective ones: formal requirement for end users to change passwords periodically, formal rule(s) regarding how passwords can be made, and formal policy governing the use of personally owned devices by government officials and employees.

If your local goverment developed any of the following, how would you rate the effectiveness of each?



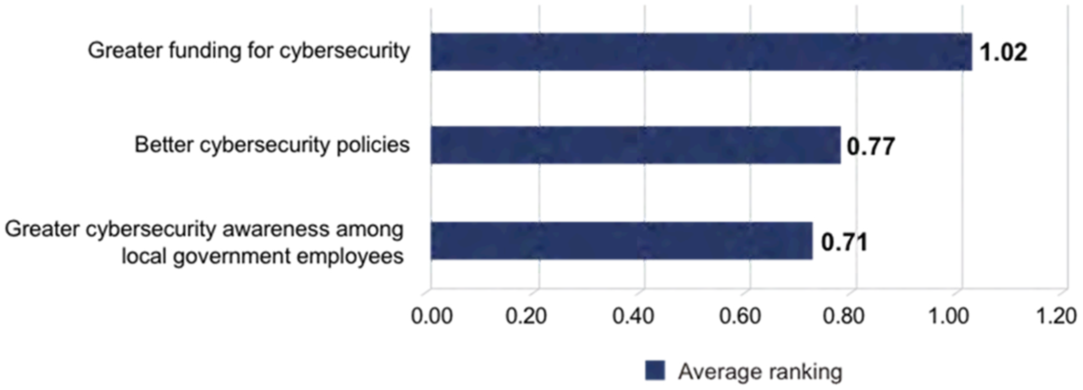
Other local governments (42.5%), vendors (40.8%), and the FBI (40.1%) were rated as extremely or very important by the responding local governments in terms of learning about cybersecurity problems and best practices. Other local governments were rated more important among counties compared to municipalities in learning about problems and best practices.

Please rate the following in terms of their relative importance to your local government's cybersecurity staff for learning about cybersecurity problems and best practices.

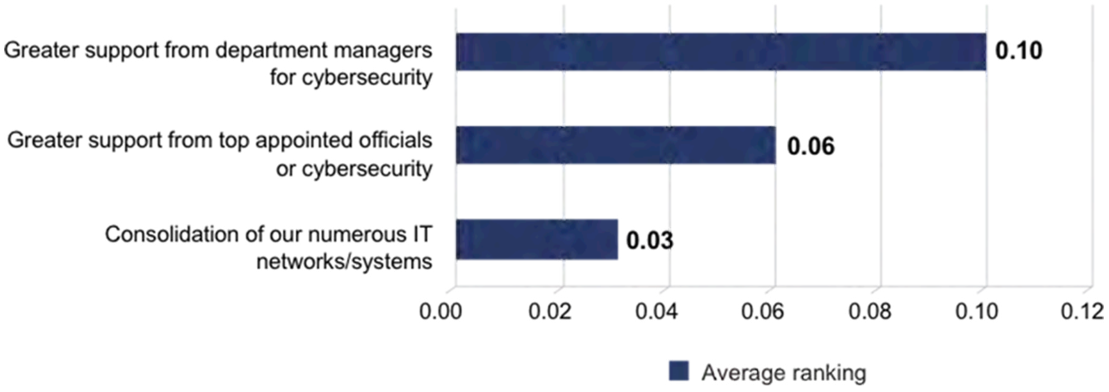


Greater funding for cybersecurity, better cybersecurity policies, and greater cybersecurity awareness among local government employees were rated as the most important things to ensure the highest level of cybersecurity among responding local governments, whereas consolidation of numerous IT networks/systems was rated as the least important one.

Top 3 things that local governments need most to ensure the highest level of cybersecurity



Top 3 things that local governments need the least to ensure the highest level of cybersecurity



Appendix A-2: Cybersecurity 2016 Survey[1]

Where is the primary responsibility for cybersecurity located in your local government's organization? (Please select one).

n=400	
Within the information technology department or related unit	**89%**
Within the elected chief executive's office (e.g., mayor, county executive)	**2%**
Within the top appointed manager's office (e.g., city or county manager or administrator)	**3%**
Stand-alone cybersecurity department or unit	**1%**
Other department, unit, or office	**5%**

Does your local government outsource any of its cybersecurity functions?

n=401	
Yes, we fully outsource cybersecurity	**8.2%**
Yes, we partially outsource cybersecurity	**29.9%**
No, we do not outsource cybersecurity	**61.8%**

If yes, to what office or official in your local government does the contractor(s) to whom you outsource cybersecurity report? (Select all that apply.)

n=153	
Information Technology Department	**50.3%**
Chief Information Officer or Information Technology Director	**32.0%**
Chief Information Security Officer	**9.8%**
Chief Technology Officer	**2.6%**
The elected chief executive's office (e.g., mayor, county executive)	**4.6%**
The top appointed manager's office (e.g., city or county manager or administrator)	**13.1%**
Other department, unit, or office	**13.1%**

See full dataset for open-ended responses for "Other department, unit, or office" option.

For the purposes of this survey, we use the following terms: ***attack, security incident (or incident), and data breach (or breach).*** We define ***attack*** as an attempt by any party to gain unauthorized access to any component of your local government's information technolo=gy system for the purpose of causing mischief or doing harm. We use Verizon's definitions of incident and breach (*2015 Data Breach Investigations Report*). According to Verizon, an ***incident*** is "Any event that compromises the confidentiality, integrity, or availability of an information asset." A ***breach*** is "An incident that resulted in confirmed disclosure (not just exposure) to an unauthorized party."

Does your local government catalogue and count attacks, incidents, and breaches?

a. Attacks (n= 377)				**b. Incidents (n= 377)**				**c. Breaches (n= 373)**			
Yes:	**46.4%**	No:	**53.6%**	**Yes:**	**58.1%**	No:	**41.9%**	Yes:	**60.1%**	No:	**39.9%**

If you answered yes to any of the options above, please indicate whether your local government employs a formal system of cybersecurity management, or if you catalogue and count the attacks, incidents, and breaches informally. (Please select all that apply.) (n= 244)

n=400	
Formal system (Please name or describe the formal system):	**31.1%**
We do this informally (Please briefly describe how you do this):	**66.4%**

How frequently is your local government's information system subject to attacks, incidents, and breaches? (Please select one from each column.)

a. Attacks (n= 366)		b. Incidents (n= 367)		c. Breaches (n= 363)	
Hourly or more	**26.0%**	Hourly or more	**4.1%**	Hourly or more	**2.8%**
At least once a day	**18.0%**	At least once a day	**4.9%**	At least once a day	**2.2%**
At least once a week	**7.7%**	At least once a week	**5.7%**	At least once a week	**1.1%**
At least once a month	**6.6%**	At least once a month	**10.4%**	At least once a month	**0.8%**
At least once a quarter	**4.6%**	At least once a quarter	**13.4%**	At least once a quarter	**3.3%**
At least once annually	**3.8%**	At least once annually	**16.3%**	At least once annually	**14.0%**
Other	**5.7%**	Other	**15.5%**	Other	**34.7%**
Don't know	**27.6%**	Don't know	**29.7%**	Don't know	**41.0%**

In the past 12 months, has your local government's information system experienced more, less, or about the same number of attacks, incidents, and breaches?

	A lot fewer	Fewer	Same	More	A lot more	Don't know
a. Attacks (n=368)	3.8%	3.8%	34.2%	22.0%	10.3%	25.8%
b. Incidents (n=365)	4.7%	8.5%	41.1%	14.8%	3.3%	27.7%
c. Breaches (n=363)	8.0%	5.2%	45.7%	3.9%	1.7%	35.5%

What percentage of attacks against your system in the past 12 months were initiated internally (that is, by employees or other persons from within your local government) versus externally (from outside your local government)? (Combined internal and external total should equal 100%.) n= 332

Average Internal		Average External		Don't know	
No.	%	No.	%	No.	%
226	**11.24%**	226	**88.76%**	106	**31.9%**

What percentage of the breaches experienced by your local government in the past 12 months occurred because end users fell victim to a phishing or spear phishing attack and opened URLs or attachments that contained malware? n= 371

No breaches (N/A)		Percentage known		Don't know	
No.	% of n	No.	% of n	No.	% of n
167	**45.0%**	128	**34.5%**	76	**20.5%**

Average percentage reported: 65.2% (n=128)

Is your local government able to determine the types of attackers that attack your system? n= 368

Yes, can determine	**41.8%**	No, cannot determine	**58.2%**

If yes, please give the approximate percentage of total attacks in the past 12 months that were initiated by each type of attacker. (Combined total should equal 100%.) n= 113

Malicious insiders (n=110)

Mean	Median	Minimum	Maximum
1.2%	0.0%	0.0%	40.0%

External actors—individuals (n=109)

Mean	Median	Minimum	Maximum
34.8%	25.0%	0.0%	100.0%

External actors—organizations (n=109)

Mean	Median	Minimum	Maximum
35.7%	25.0%	0.0%	100.0%

State actors—national governments (n=109)

Mean	Median	Minimum	Maximum
11.2%	0.0%	0.0%	90.0%

Other (n=112)

Mean	Median	Minimum	Maximum
14.0%	0.0%	0.0%	100.0%

If you know or can estimate the *purposes* of the attacks that your local government experienced in the past 12 months (i.e., what the attackers were after), please give the approximate percentage of total attacks for each category. (Combined total should equal 100%.) n= 107

Private/sensitive/confidential info (n=103)

Mean	Median	Minimum	Maximum
12.4%	0.0%	0.0%	100.0%

Confidential records (n=103)

Mean	Median	Minimum	Maximum
1.8%	0.0%	0.0%	25.0%

Employee records (n=103)

Mean	Median	Minimum	Maximum
3.5%	0.0%	0.0%	100.0%

Customer/citizen records (n=103)

Mean	Median	Minimum	Maximum
2.5%	0.0%	0.0%	50.0%

Theft of money (n=103)

Mean	Median	Minimum	Maximum
8.8%	0.0%	0.0%	100.0%

Terror (n=103

Mean	Median	Minimum	Maximum
0.1%	0.0%	0.0%	10.0%

Espionage—nation state, industrial (n=103)

Mean	Median	Minimum	Maximum
0.6%	0.0%	0.0%	30.0%

Hacktivism—i.e., Anonymous group (n=103)

Mean	Median	Minimum	Maximum
10.9%	0.0%	0.0%	100.0%

Mischief (n=103)

Mean	Median	Minimum	Maximum
16.1%	0.0%	0.0%	100.0%

Revenge (n=103)

Mean	Median	Minimum	Maximum
0.1%	0.0%	0.0%	5.0%

Ransom (n=103)

Mean	Median	Minimum	Maximum
32.0%	10.0%	0.0%	100.0%

Other (n=106)

Mean	Median	Minimum	Maximum
9.0%	0.0%	0.0%	100.0%

How would you rate the cybersecurity awareness of each of the following in your local government?

Local Government Unit/ Citizens	n	Not aware	Slightly aware	Somewhat aware	Moderately aware	Exceptionally aware	Don't know
Department managers	362	2.5%	19.1%	32.3%	33.7%	8.8%	3.6%
Elected executive (if your local government has one)	313	7.7%	20.1%	26.2%	24.6%	7.7%	13.7%
Elected councilors/ commissioners, etc.	359	9.7%	30.9%	26.5%	20.9%	4.7%	7.2%
Staff of elected councilors/ commissioners, etc.	324	7.1%	24.1%	26.2%	24.4%	6.2%	12.0%
Top appointed manager (if your local government has one)	342	2.9%	11.1%	19.0%	42.7%	19.0%	5.3%
Local judges (if judiciary is part of your local government)	271	6.3%	19.9%	18.5%	14.8%	3.7%	36.9%
Staff of local judiciary (if judiciary is part of your local government)	269	6.3%	16.0%	20.4%	17.5%	4.5%	35.3%
The average end user	361	5.0%	23.8%	33.2%	29.1%	5.0%	3.9%
The average citizen	357	10.6%	36.1%	24.4%	7.6%	0.8%	20.4%
Other	94	6.4%	7.4%	7.4%	3.2%	6.4%	69.1%

How would you rate the amount of support that cybersecurity receives in your local government from each of the following?

Local Government Unit/Citizens	n	No support	Limited support	Moderate support	Strong support	Full support	Don't know
Department managers	354	4.2%	22.6%	34.7%	21.2%	12.1%	5.1%
Elected executive (if your local government has one)	284	5.3%	19.7%	26.1%	16.2%	19.4%	13.4%
Elected councilors/commissioners, etc.	349	6.3%	25.5%	28.4%	14.3%	16.0%	9.5%
Staff of elected councilors/ commissioners, etc.	305	7.2%	21.6%	26.6%	15.1%	15.7%	13.8%
Top appointed manager (if your local government has one)	329	3.3%	12.5%	23.7%	25.8%	28.0%	6.7%
Local judges (if judiciary is part of your local government)	256	9.0%	17.2%	19.9%	10.2%	8.6%	35.2%
Staff of local judiciary (if judiciary is part of your local government)	253	8.3%	17.4%	20.9%	10.3%	8.3%	34.8%
The average end user	351	6.8%	28.2%	36.8%	16.0%	6.0%	6.3%
The average citizen	341	18.5%	24.6%	16.7%	5.0%	2.3%	32.8%
Other	66	9.1%	3.0%	6.1%	6.1%	10.6%	65.2%

How frequently does your local government take any of the following actions to improve its cybersecurity practice?

Action	n	Never	At least monthly	At least quarterly	At least annually	At least every 2 years	Don't know
Scanning and testing	351	7.4%	38.2%	19.4%	19.9%	10.0%	5.1%
Risk assessment	352	13.4%	9.9%	12.5%	40.9%	16.2%	7.1%
Technical security review	351	12.0%	8.5%	16.8%	38.2%	16.5%	8.0%
Cybersecurity exercises	348	40.8%	3.7%	6.3%	25.0%	12.4%	11.8%
Audit of our cybersecurity practices	345	26.7%	2.6%	5.5%	38.6%	17.7%	9.0%
Forensic services after incidents or breaches (leave blank if no incidents or breaches)	217	42.9%	8.8%	6.9%	17.5%	3.2%	20.7%
Cybersecurity staff training	349	20.9%	8.6%	10.3%	40.1%	12.0%	8.0%
End-user training	346	29.5%	5.8%	9.5%	33.5%	11.8%	9.8%
Cybersecurity awareness training for local government employees	350	31.7%	3.1%	10.0%	35.1%	10.9%	9.1%
Cybersecurity awareness training for local government elected officials	347	50.1%	2.6%	3.2%	21.3%	8.9%	13.8%
Cybersecurity awareness training for local government information technology personnel (not including cybersecurity personnel)	347	23.3%	10.7%	10.1%	37.5%	11.0%	7.5%
Cybersecurity awareness training for local government cybersecurity personnel	339	25.1%	11.5%	13.0%	33.9%	7.1%	9.4%
Cybersecurity awareness training for citizens	339	71.4%	1.2%	0.3%	5.0%	1.5%	20.6%
Cybersecurity awareness training for contractors	341	61.9%	2.6%	1.8%	11.7%	2.1%	19.9%
Other	45	26.7%	0.0%	2.2%	4.4%	4.4%	62.2%

To what extent is each of the following a barrier for your local government to achieve the highest possible level of cybersecurity?

Barrier	n	Not a barrier	Small barrier	Modest barrier	Somewhat severe barrier	Severe barrier	Don't know
Lack of funds	348	7.5%	9.5%	27.9%	18.1%	34.2%	2.9%
Lack of support from top elected officials	345	36.8%	21.2%	20.0%	7.0%	6.7%	8.4%
Lack of support from top appointed officials	334	41.6%	20.7%	16.5%	8.1%	5.1%	8.1%
Lack of support from department managers	345	38.0%	23.5%	20.9%	9.6%	4.1%	4.1%
Lack of availability of trained cybersecurity personnel to hire	345	20.6%	15.1%	21.7%	15.7%	15.7%	11.3%
Inability to pay competitive salaries for cybersecurity personnel	343	10.5%	9.9%	12.2%	21.0%	37.3%	9.0%
Insufficient number of cybersecurity staff	342	8.8%	11.4%	21.3%	17.3%	35.7%	5.6%
Lack of adequately trained cybersecurity personnel in my local government	342	11.7%	13.7%	23.1%	19.6%	26.9%	5.0%
Lack of adequate cybersecurity awareness in organization	341	10.6%	24.3%	31.4%	16.7%	14.1%	2.9%
The federated nature of local government (separation of powers—executive, legislative, judicial)	333	41.7%	13.8%	12.9%	8.4%	9.0%	14.1%
No end-user training at all	340	32.6%	17.9%	20.0%	13.5%	12.1%	3.8%
Some but insufficient end-user training	333	22.5%	24.9%	27.6%	11.4%	8.1%	5.4%
Lack of end-user accountability	342	14.0%	21.6%	23.4%	20.5%	17.0%	3.5%
Too many IT networks/systems within my local government	341	43.7%	1.17%	12.9%	9.4%	7.0%	5.0%
Other	31	22.6%	6.5%	6.5%	6.5%	9.7%	48.4%

Has your local government developed any of the following?

Policy/Plan/Standard/Rule	n	No, not developed	Yes, developed
Formal, written cybersecurity policy, standards, strategy, or plan	346	52.3%	47.7%
Formal, written cybersecurity risk management plan	344	66.9%	33.1%
Formal, written plan for recovery from breaches	341	66.3%	33.7%
Formal, written rule(s) regarding how passwords can be made (e.g., strength, length, permitted characters, etc.)	349	22.6%	77.4%
Formal, written requirement for end users to change passwords periodically	349	22.9%	77.1%
Formal, written policy governing the use of personally owned devices by governmental officials and employees	346	38.2%	61.8%
Formal, written cybersecurity standards for contracts with vendors for cloud-based services	339	64.3%	35.7%

If so, how would you rate the effectiveness of each?

Policy/Plan/Standard/Rule	n	Very low	Low	Average	High	Very high
Formal, written cybersecurity policy, standards, strategy, or plan	151	13.2%	17.9%	46.4%	17.2%	5.3%
Formal, written cybersecurity risk management plan	103	14.6%	16.5%	44.7%	19.4%	4.9%
Formal, written plan for recovery from breaches	106	14.2%	14.2%	44.3%	21.7%	5.7%
Formal, written rule(s) regarding how passwords can be made (e.g., strength, length, permitted characters, etc.)	246	6.9%	5.3%	32.1%	37.4%	18.3%
Formal, written requirement for end users to change passwords periodically	248	6.0%	5.6%	29.0%	37.1%	22.2%
Formal, written policy governing the use of personally owned devices by governmental officials and employees	190	10.0%	11.1%	38.9%	29.5%	10.5%
Formal, written cybersecurity standards for contracts with vendors for cloud-based services	112	14.3%	9.8%	41.1%	25.0%	9.8%

How does your local government evaluate risk and security when purchasing software as a service (SaaS) or "cloud" applications? n = 335

n=335	
a. We use the Cloud Control Matrix from the Cloud Security Alliance	**2.4%**
b. We use NIST recommendations from Special Publication 800–144	**13.1%**
c. We develop our own security and risk procedures for cloud	**24.2%**
d. We rely upon contracts to shift the responsibility and risk to the cloud vendor	**47.5%**
e. Not Applicable, we do not purchase SaaS applications	**24.8%**
f. Other	**5.4%**
Other department, unit, or office	**13.1%**

How has your local government's annual cybersecurity investment in any of the following changed over the past 5 years?

Policy/Plan/Standard/Rule	n	Decreased greatly	Decreased slightly	About the same	Increased slightly	Increased greatly	Don't know
Investment in technology (hardware, software, etc.)	347	2.3%	4.3%	31.1%	35.7%	23.1%	3.5%
Investment in additional staff	345	5.2%	6.4%	55.1%	20.6%	8.7%	4.1%
Investment in higher staff compensation	343	3.2%	7.9%	63.0%	18.4%	1.5%	6.1%
Investment in training for staff	345	4.1%	8.7%	49.0%	25.8%	7.2%	5.2%
Investment in policies and procedures	345	2.3%	5.2%	47.8%	31.0%	7.5%	6.1%

Has your local government purchased cybersecurity insurance? n=341

Yes:	**44.0%**	No:	**56.0%**

If yes, to what extent does the insurance cover your cybersecurity exposure? (Please select one.) n=152

Very little coverage	Limited coverage	Moderate coverage	Most coverage	Full coverage	Don't know
1.3%	19.7%	36.2%	17.1%	9.9%	15.8%

How would you rate your local government's cybersecurity technology (hardware, software, etc.), practices (methods used, etc.), and policies (written or unwritten "rules" or procedures, etc.)?

Technology/ Practice/Policy	n	State of the art	Current best practice	One generation behind current best practice	More than one generation behind current best practice	Don't know
Technology	344	4.9%	50.6%	29.4%	8.7%	6.4%
Practices	344	1.2%	41.9%	32.3%	18.0%	6.7%
Policies	344	0.9%	30.5%	32.0%	26.2%	10.5%

In deploying cybersecurity in your local government, are you aware of either the ISO 27000 series or the 2014 NIST Framework for Improving Critical Infrastructure Cybersecurity, and do you employ either?

Framework	n	No, not aware	Yes, aware and employ it substantially	Yes, aware and employ it partially	Yes, aware and don't employ it
ISO 27000	336	53.3%	2.4%	21.7%	22.6%
2014 NIST Framework	337	47.2%	5.0%	28.5%	19.3%

Please rate the following in terms of their relative importance to your local government's cybersecurity staff for learning about cybersecurity problems and best practices.

Institution	n	Not at all important	Slightly important	Moderately important	Very important	Extremely important	Don't know
NIST (National Institute of Standards and Technology)	335	7.8%	9.3%	21.8%	24.2%	13.1%	23.9%
FBI (Federal Bureau of Investigation)	332	8.4%	11.7%	22.9%	24.7%	15.4%	16.9%
CERT (The CERT Program of the Software Engineering Institute, Carnegie Mellon University)	332	12.7%	13.3%	18.1%	23.2%	9.3%	23.5%
DoD (Department of Defense)	328	19.5%	19.8%	16.2%	17.1%	7.0%	20.4%
Vendors	336	3.3%	15.5%	28.9%	26.8%	14.0%	11.6%
Other local governments	334	3.9%	12.0%	29.6%	27.5%	15.0%	12.0%
Our state government	333	6.9%	18.3%	24.3%	22.5%	13.8%	14.1%
Other state governments	326	23.0%	21.5%	21.5%	13.5%	4.3%	16.3%
ISO (International Organization for Standardization)	331	14.5%	18.4%	23.9%	15.1%	7.6%	20.5%
IT-ISAC (IT—Information Sharing and Analysis Center)	325	14.5%	15.1%	15.4%	13.2%	10.5%	31.4%
OWASP (Open Web Application Security Project)	327	20.8%	18.7%	13.5%	10.1%	4.0%	33.0%
MSiSAC (Multi-State Information Sharing and Analysis Center)	328	14.0%	14.9%	14.0%	12.5%	15.5%	29.0%
Other	65	7.7%	3.1%	4.6%	3.1%	20.0%	61.5%

In your experience, do the top elected and appointed officials in your local government feel that responsibility for cybersecurity belongs mostly to the technologists or do top elected and appointed officials believe that they also have to play an important role in cybersecurity? Please answer on a scale of 1 to 5, where 1 means officials believe responsibility belongs mostly to technologists and 5 means officials believe they have an important role to play.

Framework	n	1	2	3	4	5	Don't know
Top elected officials	337	51.3%	15.4%	10.7%	6.8%	2.7%	13.1%
Top appointed officials	334	42.2%	14.7%	13.8%	13.5%	3.9%	12.0%

In your opinion, what are the top three things that you need most to ensure the highest level of cybersecurity in your local government? Please select ONLY 3 and rank them in order of importance (1 = most important, 2 = second most important, and 3 = third most important). n= 319

Support	Average ranking
Improved cybersecurity hardware	0.58
Better cybersecurity policies	0.77
Better enforcement of existing cybersecurity policies	0.29
Greater funding for cybersecurity	1.02
Greater support from top elected officials for cybersecurity	0.16
Greater support from top appointed officials for cybersecurity	0.10
Greater support from department managers for cybersecurity	0.14
The ability to pay competitive salaries for cybersecurity personnel	0.38
More cybersecurity personnel	0.54
More training for cybersecurity personnel	0.42
Greater cybersecurity awareness among employees in my local government	0.71
More end-user training	0.48
Greater end-user accountability	0.32
Consolidation of our numerous IT networks/systems	0.06
Other	0.03

How confident are you that consistent implementation of the best available cybersecurity technologies, policies, and practices will enable your local government to prevent all breaches? n=334

Not confident at all	Slightly confident	Somewhat confident	Confident	Highly confident	Don’t know
13.2%	16.8%	31.1%	24.0%	11.4%	3.6%

Please share any additional information about cybersecurity in your local government.

See full dataset for open-ended responses for this question. For additional information about the Cybersecurity 2016 Survey, please contact ICMA Survey Research at surveyresearch@icma.org

Endnote

1. Certain questions were removed from the published report due to sensitivity and relevance to local government officials. If you are interested in additional information, please contact ICMA Survey Research at **surveyresarch@icma.org.**

Appendix B: Measures of Cyberattacks and Cybersecurity Preparedness

Survey data showed population size and geographic region to have strong associations with both the frequency of reported cyber attacks and cybersecurity preparedness.

Population

The frequency of cyber attacks and cybersecurity preparedness changes with the population size of a county or municipality. Both counties and municipalities with larger populations report more frequent cyber attacks, incidents, and breaches than counties and municipalities with smaller populations. Figure B.1 shows 37 percent of local governments with smaller populations (25,000—99,999) reported daily cyber attacks, while over 60 percent of local governments with larger populations (over 100,000) reported daily cyber attacks. Furthermore, approximately 80 percent of local governments with larger populations reported at least one cyber attack per year, while just over 60 percent of local governments with smaller populations did so.

These threats to local government infrastructure are not decreasing for any type of local government, but a strong correlation exists between population and change in frequency of cyber attacks. Figure B.2 shows that 67 percent of local governments with the largest populations (500,000 and up) reported an increase in cyber attacks over 2016, while 47 percent of local governments with medium-sized populations and 40 percent with smaller populations reported an increase in cyberattacks. Self-reporting is often a best-guess methodology, and these figures should be interpreted as estimates.

Figure B.1: Frequency of Cyber Attacks on Local Governments by Population

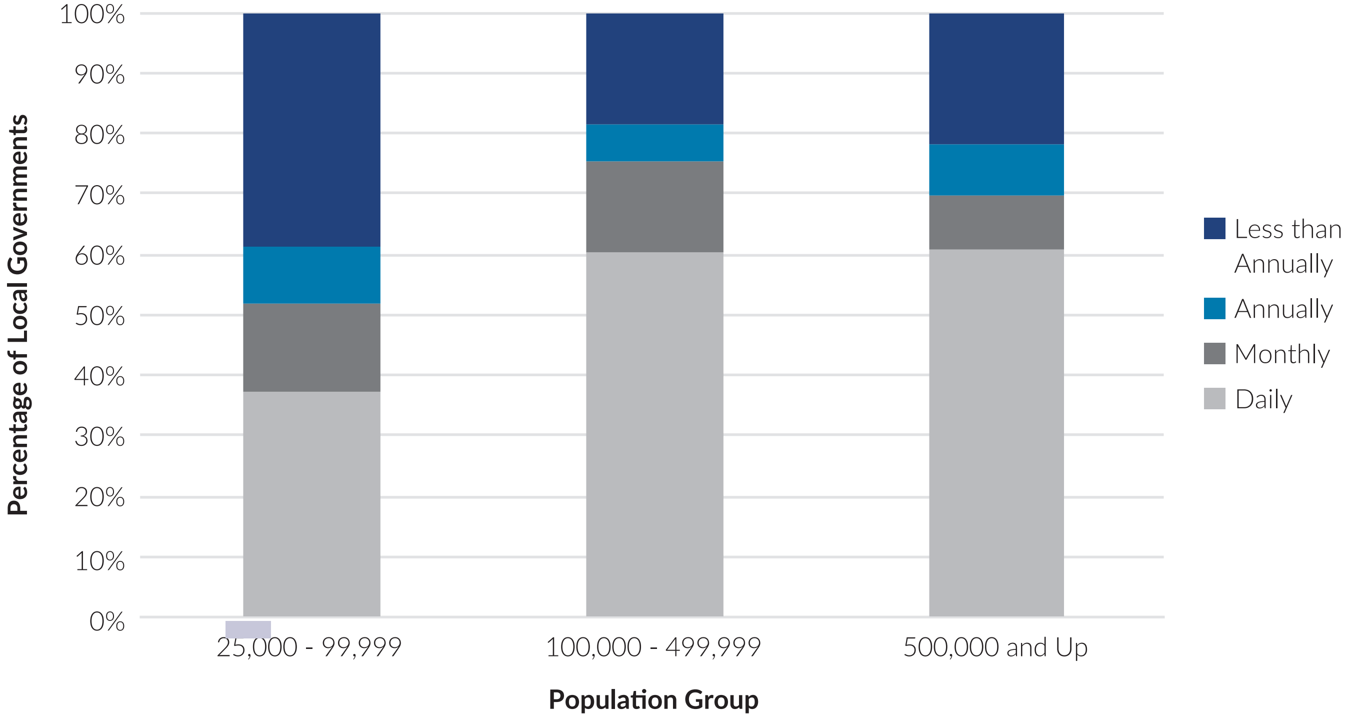
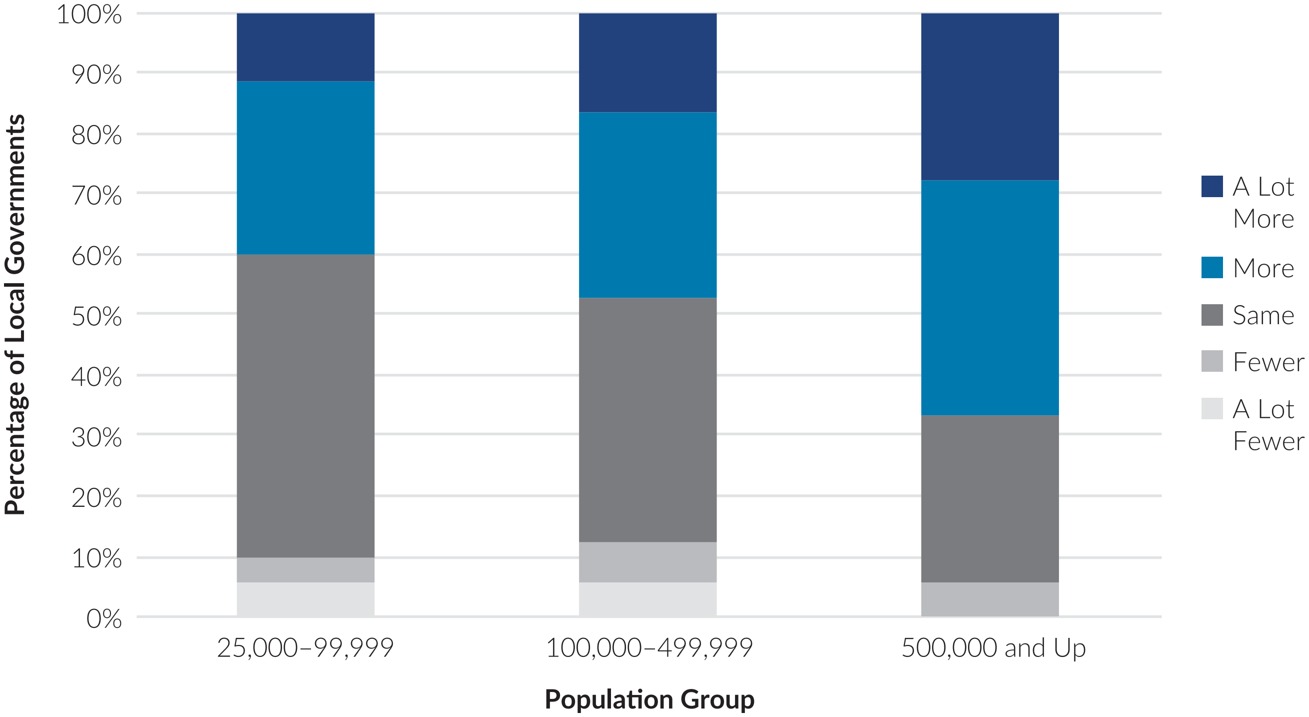


Figure B.2: Change in Frequency of Cyber Attacks on Local Governments by Population over 2016



While they experience cyber attacks more often, local government with larger populations are often better equipped to deal with these threats. Figure B.3 shows that all local governments with large populations (500,000 and up) indicated that they utilize at least four cybersecurity tools, while 95 percent with medium-sized populations (100,000—499,999) and 85 percent with smaller populations (25,000—99,999) indicated they utilize at least four tools to deal with cyberthreats. This difference dramatically increases for the use of six, seven, or eight cybersecurity tools. Local governments with large populations have an advantage in countering cyber threats over those with smaller populations because they can employ more IT and/or cybersecurity personnel. Table B.1 shows local governments with large populations (500,000 and up) have a median IT personnel size over twenty-two times larger than local governments with smaller populations, and over four times larger than those with medium sized populations. Local governments are also more likely to have multiple personnel with specific cybersecurity duties, though this advantage is not as sizable.

This relationship is flipped when it comes to rating their own cybersecurity preparedness. Table B.2 shows that local governments with medium-sized populations are more confident that their technology represents "best practice" or "state-of-the-art" than local governments with both larger and smaller populations. This is despite the fact that the number of cybersecurity tools is correlated with population, as evidenced in Figure B.3. Local governments are also less confident that their cybersecurity practices and policies are "best practice" or "state of the art."

Examples of Cybersecurity Tools in Use by Local Governments

- Anti-virus software
- Intrusion detection and prevention systems
- Web and e-mail gateways
- Network traffic analysis or network visualization
- Automated malware protection systems
- Next generation firewalls
- Multifactor/biometric authentication
- Virtual Private Networks (VPNs)

Figure B.3: Number of Cybersecurity Tools Local Governments Use by Population

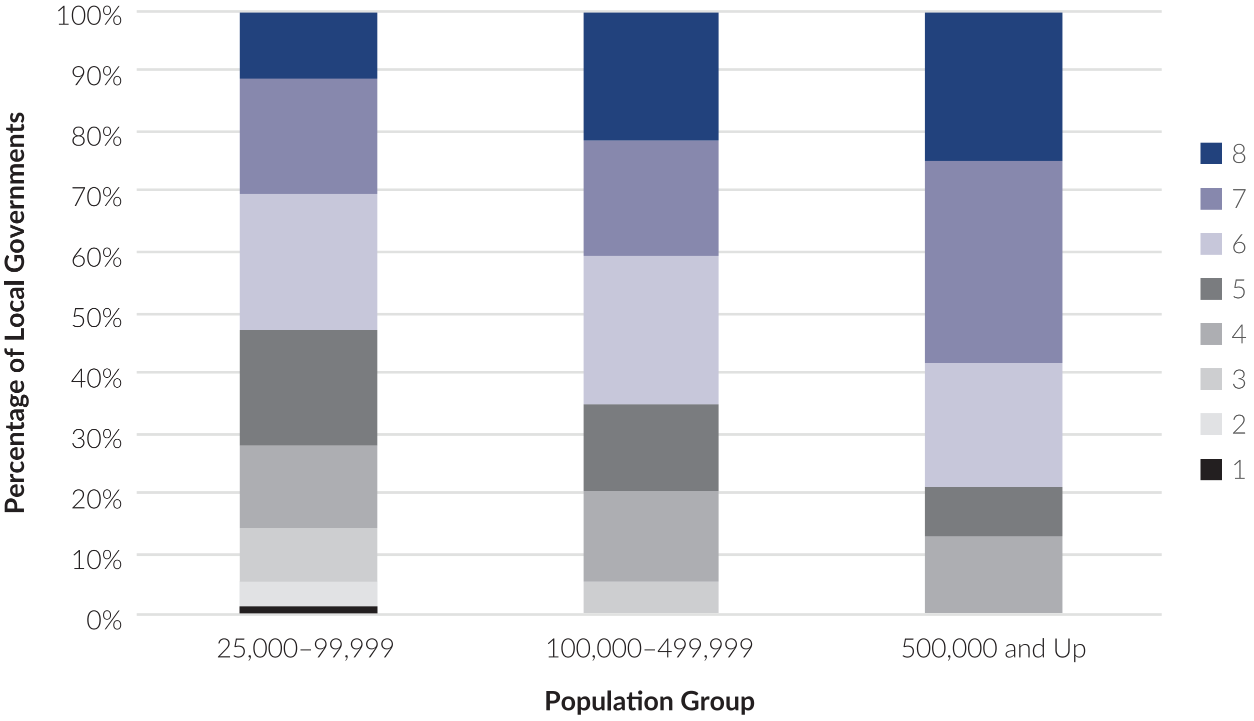


Table B.1: IT and Cybersecurity Personnel by Population

Local Government Population Size	Median IT Personnel	Percent Having Multiple Cybersecurity Personnel
25,000–99,999	5	64%
100,000–500,000	27	79%
500,000 +	113	84%
Total	7	69%

Table B.2: Local Governments with a "Best Practice" or "State of the Art" Self-Rating by Population

Local Government Population Size	Technology	Practices	Policies
25,000–99,999	54%	43%	31%
100,000–500,000	62%	44%	33%
500,000 +	50%	38%	29%
Total	56%	43%	31%

Geographic Region

Region is also a factor in the reporting of cyber attacks and cybersecurity preparedness. For the purpose of this survey, geographic region is split into two categories of the U.S. Census Bureau's regions and divisions, of which there are four and nine, respectively. Figure B.4 shows that local governments in the West region report the most frequent cyber attacks, and also most frequently reported an increase in cyberattacks as shown in Figure B.6. Local governments in the Northeast region report the least frequent cyber attacks by far, with less than half of the rate reporting daily cyberattacks as the next lest frequent region. Northeast local governments reported at least once-monthly attacks at approximately the same rate that Midwestern local governments reported at least once-daily attacks. Furthermore, while 14 percent of Northeast local governments reported hourly cyberattacks, 45 percent and 39 percent of West North Central and Pacific local governments did so, respectively.

The phenomenon of the same local governments reporting the use of more cybersecurity tools also reporting more frequent cyberattacks is repeated when holding for region. Figure B.7 shows that nearly half of Western local governments reporting using at least seven tools, while under 20 percent of Northeastern local governments utilize that number of cybersecurity tools. Once again, this is a positive relationship to the frequency of reported cyberattacks.

Additionally, as shown in Table B.3, Northeastern and Midwestern local governments have a median IT staff size half the median IT staff size of Southern and Western local governments.

Even though local governments in the West and South regions tend to utilize more cybersecurity tools than those in the Midwest and Northeast regions, employ a larger median IT staff, and are more likely to have multiple cybersecurity personnel, as seen in Table B.3, they are less likely to grade their technology as "best practice" or "state of the art," as seen in Table B.4. This trend is also seen for population size between Figure B.3 and Table B.2. It is possible that respondents interpret their answer to this question as results-based. Herein lies a paradox. The local governments generally reporting the use of fewer cybersecurity tools and "best practice" or "state-of-the-art" technologies are also reporting less frequent cyberattacks. However, the reporting of less cyberattacks could be due to fewer cybersecurity tools being in use and a less comprehensive ability to detectattacks, leading to a perception that their cybersecurity technology can be classified as "best practice" when it is not.

U.S. Census Bureau: Regions and Divisions

- Northeast
  - New England (ME, NH, VT, MA, RI, CT)
  - Middle Atlantic (NY, PA, NJ)
- Midwest
  - East North Central (MI, WI, IL, IN, OH)
  - West North Central (ND, SD, NE, KA, MN, IA, MO)
- South
  - South Atlantic (DE, MD, WV, VA, NC, SC, GA, FL)
  - East South Central (KY, TN, MS, AL)
  - West South Central (OK, AR, LA, TX)
- West
  - Mountain (MT, ID, WY, NV, UT, CO, AZ, NM)
  - Pacific (WA, OR, CA, AK, HI

Figure B.4: Frequency of Cyber Attacks on Local Governments by U.S. Census Region

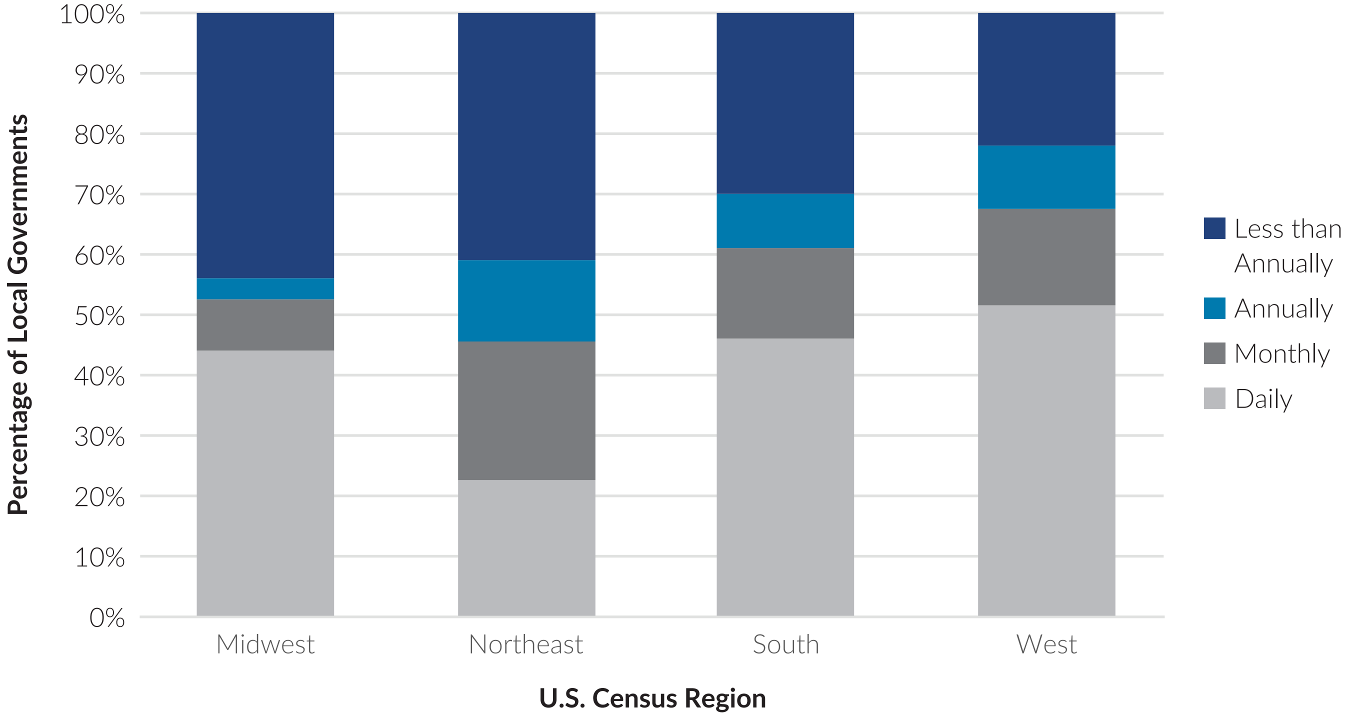


Figure B.5: Frequency of Cyber Attacks on Local Governments by U.S. Census Division

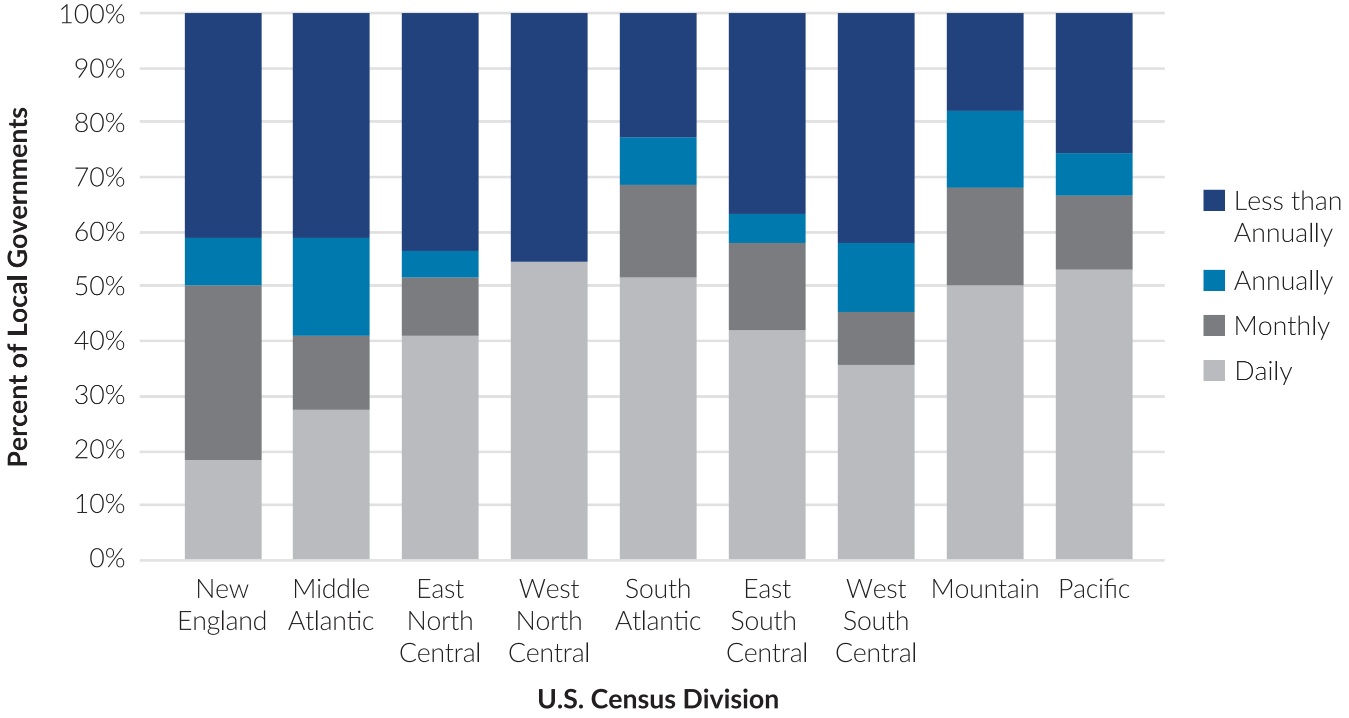


Figure B.6: Change in Frequency of Cyber Attacks on Local Governments by U.S. Census Region over 2016

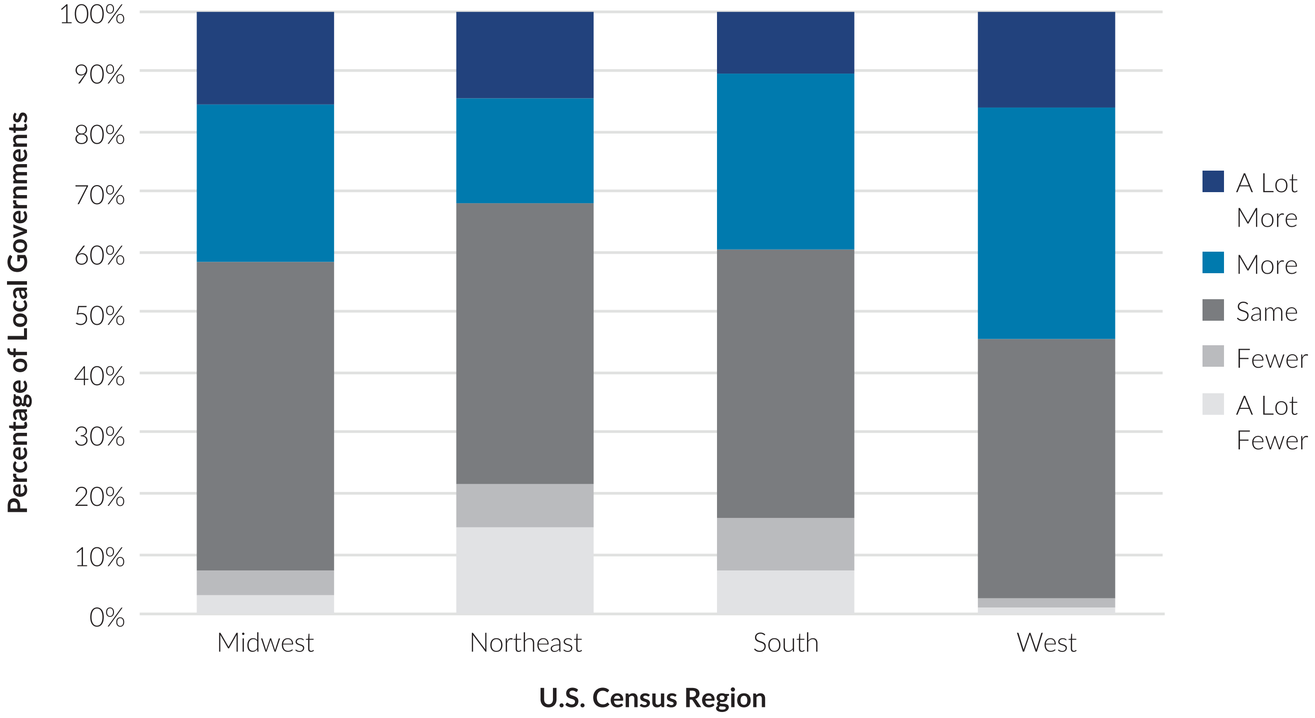


Figure B.7: Number of Cybersecurity Tools Local Governments Use by U.S. Census Region

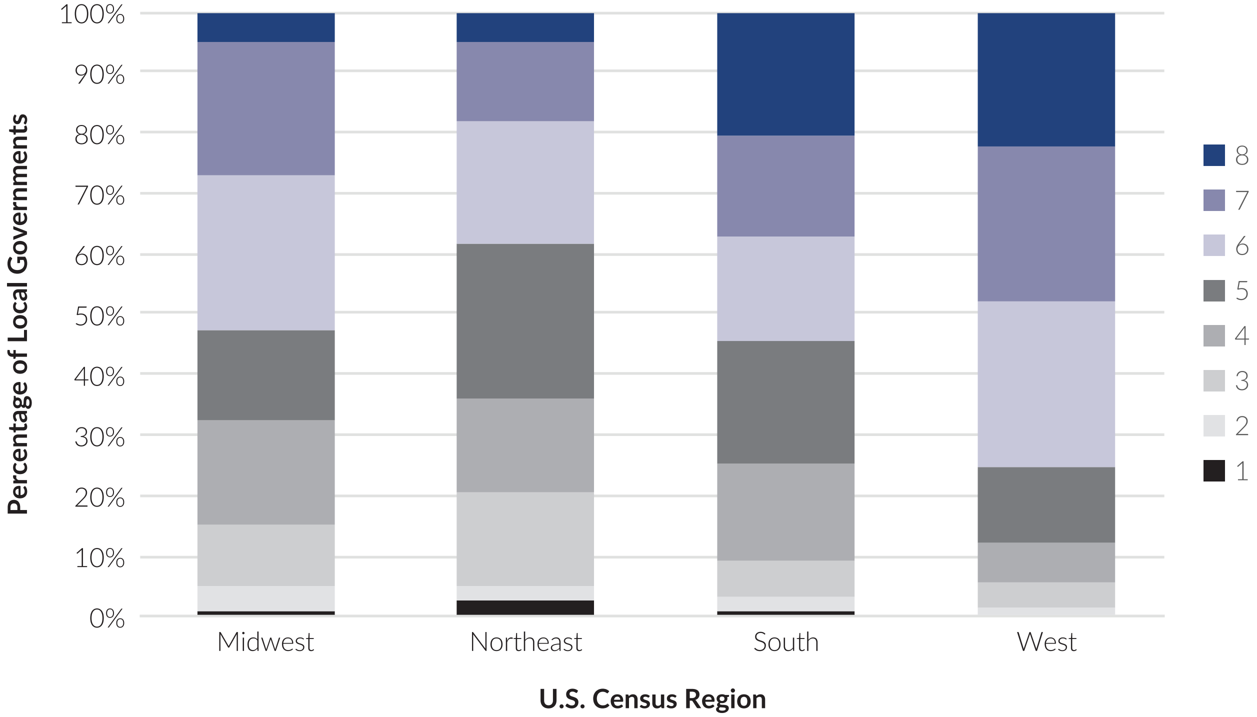


Table B.3: IT and Cybersecurity Personnel by U.S. Census Region

U.S. Census Region	Median IT Personnel	Percent Having Multiple Cybersecurity Personnel
Northeast	5	61%
Midwest	5	68%
South	11	67%
West	10	76%
Total	7	69%

Table B.4: Local Governments with a ”Best Practice” or “State of the Art” Self-Rating by U.S. Census Region

U.S. Census Region	Technology	Practices	Policies
Northeast	68%	48%	40%
Midwest	62%	45%	27%
South	53%	43%	34%
West	46%	38%	29%
Total	56%	43%	31%

Appendix C: Annotated List of Online Cybersecurity Resources

Technology Security

https://niccs.us-cert.gov/glossary
Extensive glossary of common cybersecurity terminology
Source: Department of Homeland Security (DHS)

https://niccs.us-cert.gov/acronyms
Extensive list of cybersecurity acronyms
Source: DHS

http://cybersecurityventures.com/cybersecurity-associations/
List of associations worldwide that focus on cybersecurity
Source: Cybersecurity Ventures

http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf
Guide to Information Technology Security Services
Source: National Institute of Standards and Technology (NIST)

https://ist.mit.edu/security/protecting_data
How to ensure sensitive data is protected
Source: Massachusetts Institute of Technology (MIT)

http://www.techrepublic.com/article/10-things-you-can-do-to-protect-your-data/
10 things you can do to protect your data
Source: Tech Republic

https://technet.microsoft.com/en-us/library/2007.06.securitytech.aspx
4 security technologies every IT organization must have
Source: Microsoft

www.infodev.org/infodev-files/resource/InfodevDocuments_18.pdf
Information technology security handbook
Source: InfoDev

http://www.gao.gov/assets/680/671253.pdf
Cyber threats and data breaches illustrate need for stronger controls across federal agencies
Source: United States Government Accountability Office (GAO)

http://www.gao.gov/products/GAO-08-1075R
Federal laws, regulations, and mandatory standards to securing private sector IT systems and data in critical infrastructure sectors
Source: GAO

https://www.upwork.com/hiring/development/understanding-it-security-and-network-security/
Inside IT security: How to protect your network from every angle
Source: Upwork

http://csrc.nist.gov/publications/secpubs/otherpubs/usgovII.pdf
U.S. government activities to protect the information infrastructure
Source: National Institute of Standards and Technology (NIST)

https://www.dhs.gov/blog/2011/07/22/protecting-critical-infrastructure-securing-information-technology
Protecting critical infrastructure by securing IT
Source: Department of Homeland Security (DHS)

http://ocio.wa.gov/policy/securing-information-technology-assets-standards
Securing information technology assets standards
Source: Washington State

CYBERSECURITY

https://www.dhs.gov/topic/cybersecurity
A detailed introduction about every aspect of cybersecurity
Source: DHS

http://csrc.nist.gov/
Variety of information about cybersecurity
Source: NIST

https://www.opm.gov/cybersecurity/
Government-sponsored monitoring services
Source: U.S. Office of Personnel Management (OPM)

http://www.nh.gov/doit/cybersecurity/
One-stop site for computer and Internet safety, including security updates, alerts, and resources
Source: New Hampshire Department of Information Technology

http://www.govinfosecurity.com/cybersecurity-c-223
Articles, whitepapers, interviews, and more, related to cybersecurity
Source: Gov Info Security

https://www.gsa.gov/portal/content/129686
Cybersecurity programs and policies
Source: U.S. General Service Administration (GSA)

https://its.ny.gov/local-government
Cybersecurity guide for local government staff
Source: New York Office of Information Technology Services

https://www.ffiec.gov/cyberassessmenttool.htm
Cybersecurity assessment tool for institutions and additional resources
Source: Federal Financial Institutions Examination Council (FFIEC)

https://fas.org/sgp/crs/misc/R43317.pdf
Cybersecurity: legislation, hearings, and executive branch documents
Source: Congressional Research Service (CRS)

https://www.sba.gov/managing-business/cybersecurity/top-ten-cybersecurity-tips
Top 10 cybersecurity tips
Source: U.S. Small Business Administration (SBA)

https://digitalguardian.com/blog/what-cyber-security
Definition, importance, challenges, and management of cybersecurity
Source: Digital Guardian

https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
Fact sheet: Cybersecurity national action plan
Source: The White House, Office of the Press Secretary

https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
Outline of plan to keep executive branch secure with up-to-date policies, standards, and guidelines
Source: The White House, Office of the Press Secretary

https://cltc.berkeley.edu/category/publications/
Annual report and other publications on cybersecurity
Source: Center for Long-Term Cybersecurity (CLTC)

https://www.us-cert.gov/government-users
Information sharing on cybersecurity issues among government agencies
Source: United States Computer Emergency Readiness Team (US-CERT)

https://www.fbi.gov/file-repository/cyber-incident-reporting-united-message-final.pdf/view
Cyber incident reporting—a unified message for reporting to the federal government
Source: Federal Bureau of Investigation

TOWN HALL