



## County and Municipal Cybersecurity

### The cybersecurity risk to local government

Weak or nonexistent cybersecurity programs represent a massive organizational risk to county and municipal government agencies in the United States. County and municipal executives are often unaware of these risks because they assume that their IT Director, CIO, or an external vendor is managing security and addressing the risks. It is rare that such an assumption is correct.

While the Ponemon Institute<sup>i</sup> found that “federal organizations have a stronger cybersecurity posture than state and local organizations,” the Brookings Institute<sup>ii</sup> concluded that “the vast majority of public agencies lack a clear cybersecurity plan.” Much of the available research is based on small samples and I believe that these studies may understate the scope of the problem. Based on my 23 years of working with public sector organizations, I can state with confidence that most lack any cybersecurity plans at all.

Your job as a municipal executive is to provide leadership and management in order to get the big picture right throughout your organization. What follows is advice on how to ensure that an appropriate cybersecurity program is established and functional in your organization. I recommend that you, the municipal executive, assume high-level responsibility for cybersecurity oversight. You don’t need to know the technical details, but you must know whether or not the appropriate frameworks, infrastructure, policies and procedures are in place and working correctly.

### Definitions

The need for information security is as old as civilization and possibly as old as life on earth. Information Security (Infosec) was invented to protect the first secret – whenever and whatever that was. Infosec is not solely a human artifact -- my Great Dane always felt the need to maintain security concerning the location of his favorite bones and dead woodchucks. Techniques, methods and

models for protecting information haven’t changed all that much and the methods of cybersecurity are largely based on models for protecting physical information.

Information Security refers to the discipline and processes to protect the confidentiality, integrity and availability of all your information regardless of form. Cybersecurity is a subset of *information security* and applies to digital data. In this article, I may use them interchangeably even though they are not, but counties and municipalities need an Infosec plan that includes cybersecurity.

### Municipal data – a pot of gold

County and municipal networks are treasure chests overflowing with priceless gems. Mortgage documents, deeds, births, deaths, ugly divorces, medical records, social security numbers, and military discharge documents are among the many types of publicly accessible documents that may contain PII (Personally Identifiable Information), PHI (Protected Health Information), or other sensitive information. Constituents turn over all this information naively assuming that you are doing everything in your power to protect it from theft and misuse. Are you a worthy steward of this treasure?

### Root causes and obstacles

Let’s discuss eight of many root causes of failure to establish appropriate information security programs in local government organizations. Subsequently, we’ll move on to a methodical, practical approach you can initiate immediately to improve your cybersecurity posture.

### Personnel

“A lack of skilled personnel is a challenge at both federal and state and local organizations.”<sup>iii</sup> One problem is that many public sector IT Directors and CIO’s don’t have the knowledge, training and background to plan and deliver acceptable, standard’s based comprehensive information security programs. They are often unaware of widely



accepted standards, guidelines and frameworks that are readily available, so cybersecurity planning is often amateur and homebrewed. Moreover, HR and hiring managers often don't understand the required skills<sup>iv</sup> and look for the wrong people.

The largest municipal agencies may employ a CISO (Chief Information Security Officer) but the vast majority of public sector organizations do not have a dedicated information security executive and staff, nor should they necessarily require one.

IT staff members are rarely trained in or even familiar with relevant statutory compliance requirements. I have come to expect a *deer in the headlights* look from public sector CIO's and IT staff when inquiring about security policies, privacy policies and other matters of security and compliance. Questions about HIPAA Security Rule compliance, for instance, are almost always met with "What's that?"

### ***A jumble of regulations***

Municipal organizations may have dozens of departments, divisions, or lines of business with varying regulatory requirements from numerous federal and state agencies. Municipal governments do a lot. They may be involved in building bridges, managing traffic signals, providing water, waste, electric and sewer services, supervising elections and recording deeds while providing physical and mental health services and dental care.

A typical County government may have to comply with regulations like HIPAA<sup>v</sup> (Health Insurance Portability and Accountability Act) and 42 CFR<sup>vi</sup> while also complying with policies from CJIS<sup>vii</sup> (Criminal Justice Information Systems) in addition to compliance with state regulations from organizations such as an Office of Mental Health, or Department of Health. Additional requirements for records management from State Archives agencies add to those complexities and often contradict other regulatory requirements.

### ***Shared Infrastructure***

Departments with vastly different information security and regulatory compliance requirements often coexist on a shared network where the security posture is designed for the lowest common denominator rather than for the highest. Often, municipal IT staff members don't have clearly defined policies and procedures for reviewing information such as security logs and system events. Even if they do record these events, their stance is usually reactive rather than proactive.

### ***Silos and turf wars***

Counties and municipalities may have highly distributed management structures which function as silos rather than as a cohesive team. In some states, the silos may be a "feature" of constitutional government where elected officials manage some departments and may not be accountable to central executives. One result of this is that a county executive, and consequently County IT, may not have global control of IT and information security because other elected officials choose not to cooperate. Some real world examples I have seen include:

- County Judges and their staff members refuse to sign and abide by acceptable use policies.
- County Sheriffs refusing to cooperate with an IT security audit claiming their security policy and processes are "secret."
- Social Services commissioners unilaterally declaring that HIPAA regulations don't apply to their operations.

Silos in organizations create massive gaps in security management. When multiple parties are responsible for security, no one is responsible.


### ***Most security problems are internal***

90% of breaches occur because of an internal mistake<sup>viii</sup> and 60% of breaches are a result of internal attacks<sup>ix</sup>. Unfortunately, county and municipal information security programs often treat outside threats as 100% of the problem rather than focusing on more probable internal threats.

# e-volve Information Technology Services

Municipal & Enterprise Information Technology Services



Information & IT Governance  Information Security & Cybersecurity

e-mail: [jmorgan@e-volve.com](mailto:jmorgan@e-volve.com)  
Phone: (607) 731.4097

Audits and Assessments • Strategic Planning • Enterprise Software Procurement • Business Process Reengineering  
Project & Implementation Management • Regulatory Compliance • IT Service Management • Virtual CIO

## **Budget**

Insufficient budget is often used as an excuse for low quality IT services and lack of security in public sector organizations. It's usually a red herring. In my experience, there is no correlation between budget and quality in the public sector. I have seen small, low-budget organizations build excellent security programs and have also seen large organizations with eight-figure tech budgets fail to establish even the most elementary components of an information security program. A cybersecurity program will cost money, but it doesn't have to bust your budget.

## **Political Hiring**

In local government, critical management positions are often filled based on political considerations rather than quality of candidates. Expertise in information security should be a major component in your CIO's toolkit.

## **Tech versus strategic thinking**

If you think in terms of technology, *stop it!* I am always a little suspicious of industry professionals who fall in love with a particular technology. Technology is rapidly replaced or superseded so think strategically instead. There is no such thing as a technology problem; there are only business problems. Identify and solve for the business problem and the appropriate technical solution will reveal itself.

## **Start with Information Governance (IG)**

What's the first step in establishing your cybersecurity program? It has nothing to do with cybersecurity.

Information Security and cybersecurity must be components of your overarching **Information Governance (IG) Program**, overseen by an interdisciplinary team with executive support. Treating cybersecurity as a standalone program outside of the context of your organization's information universe will produce a narrow approach. Do you currently have an IG program?

I can hear some grumbling right now. "Jeff, when do we get to the important stuff?"

IG *is* the important stuff. There are no silver bullets. There are no miracle pills that will address your information security requirements. No miraculous hardware or software will magically keep your information safe unless you have the right policies in place. There is some real work to do here and the P-things are the most effective tools to pack for your InfoSec journey. You will develop these from your IG Program:

**Policies • Processes • Procedures**

**Protocols • People**

## **What is information governance?**

I like Robert Smallwood's succinct definition of Information Governance: "security, control and optimization of information."<sup>1</sup> In order to develop sound InfoSec and cybersecurity programs, you must know what you are protecting and why you are protecting it. The purpose of the IG program is to map, understand and manage your entire information universe. The map you create will serve as the foundation for your information security programs.

In a municipal government organization, an IG committee may include legal, HR, records management, IT, finance, and auditors, as well as other departments. Let's say your municipality has a public health clinic, recorder of deeds, personnel/payroll and a sheriff. This means you have medical records, prisoner health records, recorded 911 calls, police reports, mortgage documents, confidential personnel records, payroll records, social security numbers and a lot more. The people with special knowledge about the nature and disposition of all this information must be on your committee.

In some organizations, information and security policy is developed at the whim of the CIO or IT Director. Is that IT Director expert in statutory requirements and industry best



practices for all the areas mentioned above? I doubt it. This is why you need a cross-functional team to map the universe and make a comprehensive plan.

### Establishing a comprehensive information security program

Once you have begun building your IG foundation and framework, your Infosec and cybersecurity requirements will be much clearer. Also, IG, Infosec, and Cybersecurity are not one-time activities. They require a process for continuous improvement like PDCA (Plan, Do, Check, Act) or DMAIC (Define, Measure, Analyze, Improve, Control). Get something in place first, and then continue to improve it. Attempting to get it perfect from the start will only result in implementation delays. This job never ends but it gets much easier once a solid foundation has been built.

### Information Security Management Systems (ISMS), Frameworks and Standards

Once you have a comprehensive understanding of your information universe, develop security policies and programs for implementation and enforcement of those policies.

**Use an existing framework.** Designing comprehensive information security programs is more complicated than installing firewalls and anti-virus software and there is a great deal to think about.

There are many freely available information security tools in addition to standards and frameworks that require payment or membership in an organization. You can build a successful security program using only free tools, but my crystal ball is on the fritz today so I can't see which tool is best for your organization. I wish I could tell you there is a one-stop shop, but there isn't. You will have to evaluate your situation, do the research and make informed decisions about the best approach for your organization. Following is a brief discussion of some of them.

### NIST

The **National Institute of Standards and Technology** ([NIST](#)) provides an enormous quantity of information and the gateway to it is available [here](#). NIST's *Framework for Improving Critical Infrastructure Cybersecurity* is available [here](#) and a new draft was released in January of 2017. Their [Cybersecurity Framework Workshop](#) starts on May 16, 2017 in Gaithersburg, MD if you would like to attend and learn more about it. You can also view a [webcast](#) with an overview of the *Framework*. In their words, "The core of the framework was designed to cover the entire breadth of cybersecurity . . . across cyber, physical, and personnel."<sup>1</sup>

NIST also provides three Special Publication (SP) series: SP800 deals with Computer Security, SP1800 contains Cybersecurity Practice Guides, and SP500 covers Computer Systems Technology.

[SP800-53](#), *Security and Privacy Controls for Federal Information Systems and Organizations* will likely be an essential part of your planning process if you are building upon NIST.

### HIPAA

If a division of your public sector organization provides clinical services, it might fit the definition of a [covered entity](#) (CE). If so, that division is required to comply with applicable federal regulations including the [HIPAA Security Rule](#). The regulation provides a clear, jargon-free framework for developing information security policies and programs. While it won't address all the requirements for a municipal cybersecurity program, it can help you build a solid foundation for your security programs. I don't have any official data on HIPAA Security Rule compliance in municipal organizations, but my personal experience is that it is extremely low. Is your CE compliant? If not, why not bring your entire organization up to HIPAA standards?

I have worked extensively with HIPAA regulations and NIST products for nearly 2 decades and I like them a lot.



# e-volve Information Technology Services

Municipal & Enterprise Information Technology Services



Information & IT Governance  Information Security & Cybersecurity

Audits and Assessments • Strategic Planning • Enterprise Software Procurement • Business Process Reengineering  
Project & Implementation Management • Regulatory Compliance • IT Service Management • Virtual CIO

e-mail: [jmorgan@e-volve.com](mailto:jmorgan@e-volve.com)  
Phone: (607) 731.4097

If they are not a good fit for your organization, there are other resources, including the following three.

## ISF

The **Information Security Forum (ISF)** publishes the *Standard of Good Practice for Information Security*, available free to ISF members.

## ISO

The **International Organization for Standardization (ISO)** publishes the [ISO/IEC 27000](#) family of standards for Information security management systems. ISO products are not inexpensive, but in the overall scheme of things you might find them to be a reasonable investment. Organizations can certify through accredited registrars, which can also be an expensive process.

## ISACA

ISACA publishes [COBIT5](#), "the leading framework for the governance and management of enterprise IT" which provides an integrated information security framework as part of a larger IT governance framework. According to Joseph Granneman, "It is the most commonly used framework to achieve compliance with Sarbanes-Oxley rules."<sup>xiii</sup>

## The role of vendors

Trusted vendors can be helpful in building your programs, but overreliance on vendors for security advice is a suboptimal approach. While they may be knowledgeable about many aspects of your industry, only you and your cross-functional IG team truly understand your business requirements. Their job is to "sell you stuff" but they will generally draw the line at writing policy and taking responsibility for overall information security in your organization. If there is a major breach or some other catastrophic security event in your organization that becomes public, you are the one whose picture will be in the paper.

## Summary - one step at a time

Take a few simple steps to improving your cybersecurity infrastructure:

1. Establish an IG committee and program.
2. Discover and map your information universe.
3. Establish an information security framework and security policy.
4. Develop and implement your cybersecurity plan, based on the above.
5. Use a cycle of continuous improvement.

## Note:

This article first appeared in two parts in my [CIO.COM](#) column at:

[County and Municipal Cybersecurity Part 1](#)

[County and Municipal Cybersecurity Part 2](#)

A continuation of the subject appeared in:

[Hippa as an Umbrella for County/Municipal Cybersecurity](#)

## References, Resources and Further Reading

[Four critical challenges to state and local government cybersecurity efforts](#). Government Technology. July 17, 2015.

[The need for greater focus on the cybersecurity challenges facing small and midsize businesses](#). Commissioner Luis A. Aguilar, October 19, 2015. US Securities and Exchange Commission.

[How state governments are addressing cybersecurity](#). Brookings Institution. Gregory Dawson and Kevin C. Desouza. March 2015.

[World's oldest hacking profession doesn't rely on the internet](#). CNBC

[Four critical challenges to state and local government cybersecurity efforts](#). Government Technology. July 17, 2015.

[Human error is to blame for most breaches](#). Cybersecuritytrend.com.

# e-volve Information Technology Services

Municipal & Enterprise Information Technology Services



Information & IT Governance  Information Security & Cybersecurity

Audits and Assessments • Strategic Planning • Enterprise Software Procurement • Business Process Reengineering  
Project & Implementation Management • Regulatory Compliance • IT Service Management • Virtual CIO

e-mail: [jmorgan@e-volve.com](mailto:jmorgan@e-volve.com)  
Phone: (607) 731.4097

[Cisco 2017 Annual Cybersecurity Report.](#)


## Endnotes

- <sup>i</sup> [The state of cybersecurity in local, state and federal government.](#) Ponemon Institute. October 2015.
- <sup>ii</sup> [The vast majority of the government lacks clear cybersecurity plans.](#) Brookings Institution. February 3, 2015. Kevin C. Desouza and Kena Fedorschak.
- <sup>iii</sup> [The state of cybersecurity in local, state and federal government.](#) FCW.
- <sup>iv</sup> [Cybersecurity unemployment rate at zero.](#) SC Magazine. Doug Olenick. September 2016.
- <sup>v</sup> [HIPAA Security Rule, Combined Text.](#)
- <sup>vi</sup> [42 CFR Part 2.](#)
- <sup>vii</sup> [CJIS Security Policy Resource Center](#)
- <sup>viii</sup> [IBM X-Force 2016 Cyber Security Intelligence Index](#)
- <sup>ix</sup> [The biggest cybersecurity threats are inside your company.](#) Harvard Business Review. Marc van Zadelhoff. September 19, 2016.
- <sup>x</sup> [Information Governance for Executives.](#) Robert Smallwood. 2016 Bacchus Business Books.
- <sup>xi</sup> [National Institute of Standards and Technology.](#)
- <sup>xii</sup> [IT security frameworks and standards: Choosing the right one.](#) Joseph Granneman, Techtarget.com. September 2013.

## More Information

If you found this information useful, or would like to discuss cybersecurity in your organization in more detail, please feel free to e-mail me at [jmorgan@e-volve.com](mailto:jmorgan@e-volve.com). I would be glad to discuss your situation.

## e-volve Information Technology Services, LLC

About the Company	Contact me!
 <b>e-volve</b> provides transformational Technology and Management Consulting services to <b>improve business performance</b> while <b>lowering costs</b> . We provide standards'-based <b>Information Technology Governance</b> services and sell neither hardware nor software. We are technology-neutral, receive no commissions from vendors and provide services anywhere in the Continental United States.	e-mail: <a href="mailto:jmorgan@e-volvellc.com">jmorgan@e-volvellc.com</a> Voice: (607) 731.4097 Blog: <a href="http://blog.e-volvellc.com">http://blog.e-volvellc.com</a> LinkedIn: <a href="https://www.linkedin.com/in/evolvejrmorgan">https://www.linkedin.com/in/evolvejrmorgan</a> <b>e-volve Information Technology Services, LLC</b> 519 Blakeslee Road Milan, PA 18831

### About Jeffrey Morgan

I have provided business and management consulting services to County and Municipal Governments, Large/Medium/Small Businesses, and Nonprofits since 1993. I write extensively on IT Governance, management, and organizational culture for CIO.COM, Careers in Government, and other publications. My book, *Enterprise Software Procurement: Tools and Techniques for Successful Software Procurement and Business Process Engineering for Municipal Executives and Managers* is available from Amazon.

### Industry Standards & Best Practices

I approach business and technology problems using widely accepted industry standards and frameworks including ITIL, ISO20000, PMBOK, Agile, NIST, ANSI/EIA/TIA, and others in order to achieve measurable goals and objectives while focusing on Quality, Total Cost of Ownership, and Return on Investment.

### Services

#### Enterprise Services, Information Governance, IT Governance

- Municipal and Enterprise Software Procurement & Implementation including ERP, CRM, EHR, Public Safety, PSA, ERMS, Case & Document Management, and more.
- Enterprise Network Architecture.
- RFP's, SOW's, SLA's and Contract Negotiations.
- Business Process Assessments & Reengineering.
- Project Management.

#### Information Security

- Information Security Audits, Risk Assessments, and Regulatory Compliance including HIPAA and FFIEC.
- Information Security Policy & Procedure Development.
- Information Security Design and Architecture.

#### Audits and Assessments

- Information Technology Audits and Assessments.
- Business Process & Regulatory Compliance Audits and Assessments.

#### Virtual CIO and Management Consulting

- Strategic Planning.
- Executive Advisory Services.
- IT Staff Reorganization & IT Services Design.
- Outsourcing Contracts.
- Policy and Procedure Development.