e-volve Enterprise Management Services
for Local Governments and Behavioral Health

• Management Advisory Services • Enterprise Projects • Business Process Reengineering
• Information Security • Digital Transformation • Research • Special Projects

e-volve
607.731.4097
jmorgan@e-volvellc.com

County and Municipal Executive's Guide to Cybersecurity

A resource guide to information and cybersecurity for local government directors, executives, and managers

Jeffrey Morgan
President, e-volve Enterprise Management Services

Reading Time – 20 minutes

e-volve

© Copyright 2019, Jeffrey Morgan

Contents

Cybersecurity Myths 3
Why should municipal executives care about cybersecurity? 3
Information and cybersecurity problems cost money. 3
Cybersecurity incidents are a reflection of organizational management. 3
What fails in cybersecurity incidents and breaches? 4
How would you handle a breach? 5
Should cybersecurity programs be built on technology? 5
Is cybersecurity an IT responsibility? 5
Major components of a cybersecurity program 6
Standards, Frameworks, and Regulations 7
ISO/IEC 27001 7
NIST Framework for Improving Critical Infrastructure Cybersecurity 7
HIPAA Security Rule 7
Action Plan - How to build a cybersecurity program – first steps 8
How much work does it require? 8
How much does it cost? 9
Getting Help 9
Ready to talk? Contact us! 9
Read my other publications 9
Information Security Articles 9
Governance and Management Articles 10
References 10

Cybersecurity Myths

Information and cybersecurity are somewhat mythical subjects and many misconceptions abound. Here are a few examples of the many myths surrounding cybersecurity:

1. Information and cybersecurity programs are built on technology.
2. Cybersecurity programs are expensive.
3. Information and cybersecurity programs should be managed by Information Technology staff.
4. The greatest cybersecurity threats come from outside your organization.
5. Your IT staff would be able to detect a breach or other anomaly.

Do you believe in any of these myths? If so, keep reading because all five of these statements are false.

Why should municipal executives care about cybersecurity?

Information and cybersecurity problems cost money.

According to the 2018 Ponemon Institute Data Breach Study[i], the average total cost of a data breach is $3.86 million. Data breaches aren't the only type of devastating cybersecurity problem and global costs for ransomware are expected to reach $11.5 billion[ii] in 2019. Malware can quickly bring a halt to your business activities and we have seen municipal services brought down for over a week because of infections that were a result of failure to follow policies and procedures.

Non-fiscal consequences of information security problems may have a more significant long-term impact on your organization than fiscal consequences and may include loss of reputation and litigation.

Cybersecurity incidents are a reflection of organizational management.

Information Security disasters are almost always a reflection on organizational management and the worst time to find out that you didn't have a comprehensive cybersecurity program is in the aftermath of a breach. Most cybersecurity events occur for one of three reasons:

1. People didn't do what they were supposed to do (i.e. patching, backing up, checking logs).
2. People did something they weren't supposed to do (i.e. using inappropriate web sites, inserting flash drives, opening links on phishing e-mails).
3. People have no idea what they are supposed to do (lack of policy, procedures throughout the organization).

Knowing what your staff is doing is a basic management responsibility. Show me a cybersecurity incident, and I will show you a chain of supervision and management failures that go all the way to the top of an organization.

Boards and governing bodies are beginning to see it this way too, and currently, senior C-level executives lose their jobs in roughly one-third of breaches[iii] and other cybersecurity events.

Quite simply, information and cybersecurity are management responsibilities and good information security programs require ongoing management attention. Managers don't need to be cybersecurity or technical experts; they do need to ensure that appropriate controls, policies, and procedures are in place. Your IT department isn't the solution; management principles are.

What fails in cybersecurity incidents and breaches?

Depending on what research you read, somewhere between 60 and 90 percent of cybersecurity problems are caused by human error. In my experience, 90 percent sounds about right, although it could easily be closer to 100 percent. This all fits right in with W.E. Deming's theory that 94% of problems in an organization are a result of management failures.

Major information breaches occur daily and only a small percentage of these make headline news. The most infamous of these include Equifax, Marriott, Yahoo, Target, and Anthem. In many local governments and smaller enterprises, the cybersecurity programs are not sufficiently robust to even identify whether a breach has even occurred.

A small sampling of 2018 information security incidents from the county and municipal sectors includes:

1. City of Atlanta
2. St. Lawrence County, New York
3. Adams County, Wisconsin
4. Otsego County, NY
5. 50 central New York school districts

What most breaches have in common is that technology didn't fail – people failed. Policies, procedure, and management failed. In the Equifax breach, someone failed to apply current patches to servers with known vulnerabilities. The CEO, Richard Smith, lost his job over the incident, but he wasn't the culprit who failed to patch. He did handle the incident poorly, though.

If you take a proactive approach to cybersecurity, you have control over what you do and how you do it. However, in the aftermath of a breach, you may find your organization under investigation by the US Office of Civil Rights if the breach involved PHI and criminal charges may be involved as well. Your response may be dictated by state and federal regulators and you will have lost control of the process. A proactive approach to cybersecurity is clearly more desirable.

How would you handle a breach?

How would your organization be able to identify a breach? In the case of Adams County, WI the breach went on undetected for over five years and resulted in the disclosure of PHI and PII of over 250,000 residents. Five years! Would your staff be able to detect a breach?

Would you know how to respond to a breach? When it comes to cybersecurity, you must know how to respond to disasters before they happen and developing an incident response plan is part of the process of building a comprehensive information security program. A disciplined approach forces you to think about everything so that when a disaster of some sort does occur, you are prepared to deal with it immediately. However, if you have taken a comprehensive approach to cybersecurity, a disastrous problem is far less likely to occur. And, if it does occur, the response and cleanup is considerably easier.

Should cybersecurity programs be built on technology?

Most information and cybersecurity programs are caused by people, so why are most cybersecurity programs built on technology? The foundation for a great cybersecurity program is policy and procedure.

Often, when I talk to executives and managers, their response to information from me is something like, "Wow. This is great information. I'll show it to my IT people." This is a pretty clear indication that they didn't hear anything I just presented. This is understandable; most managers have been conditioned to believe that information security is an IT responsibility.

As an executive, you will be held accountable for a serious cybersecurity incident, especially if the problem was caused by lack of policy, procedure, and management oversight.

Is cybersecurity an IT responsibility?

The conventional wisdom in local governments is that information and cybersecurity are functions that should delegated to an IT Director or CIO. As is the case with most conventional wisdom, this view is wrong.

Cybersecurity is often treated as a form of black magic where wizards practice their secret arts in the data center. In reality, the processes, procedures, and activities that your staff should be performing routinely are well-known and widely published. Are your staff members following these publicly available standards?

Over the last several decades, many comprehensive standards and frameworks for information and cybersecurity have grown and matured. These frameworks have been developed by large workgroups of brilliant people who have devoted their professional careers to the study of information security. Local governments rarely implement these frameworks and instead rely on ad hoc programs designed by staff members untrained in information security practices and procedures. None of these standards or

frameworks recommends delegation of cybersecurity to IT staff; all of them recommend comprehensive approaches that include the participation of directors, executives, and senior managers in building a comprehensive plan.

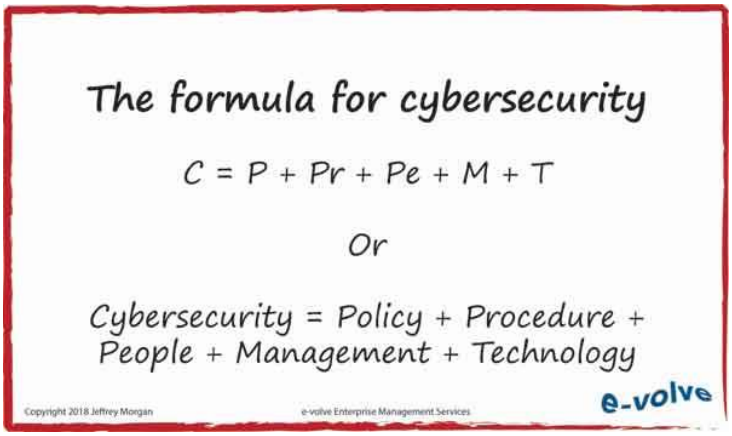
The good news is that this problem is simple to fix. Building a solid, standards-based cybersecurity program is a team effort and the majority of controls that should be implemented are not technical in nature, but administrative.

Major components of a cybersecurity program

How do you know if you have a standards-based cybersecurity program or an ad hoc one? It is easy to identify a real cybersecurity program and six elements distinguish a comprehensive program from a poor one:

1. **Comprehensive Security Policy.** For most municipal governments, this document should probably consist of 25 or more pages and at least 40- 50 policies, but probably many more. Good security policies are typically developed over a long period of time
2. **Acceptable Use Policy.** This document describes standards for using company-owned resources, ownership, reporting requirements, etc. but may also address the use of social media, work-at-home policies, and a great deal more.
3. **Risk Assessment Report.** Risk assessments are a requirement of every standards-based security framework. If you don't have a relatively current risk report, your security program doesn't meet the standards of any generally accepted information security framework.
4. **Documentation.** Extensive documentation demonstrating compliance with your organization's security policy should be readily available at all times. Do you have evidence that backups are validated? Are logs checked? Excellent documentation is a required component of a true information security program.
5. **Management participation.** Participation of directors and senior managers in an information security program is a requirement. For most county and municipal governments, managing and understanding the scope of information and the regulatory requirements are beyond the knowledge, skills, and abilities of the IT staff.
6. **Accountability.** A good cybersecurity program requires participation of staff and management throughout the organization. Responsibility and accountability for the many tasks must be clearly documented so everyone understands their part.

There are many moving parts to a good cybersecurity program and the formula for it looks something like this:



Standards, Frameworks, and Regulations

There is no reason for the existence of ad hoc information security programs, especially in the public sector. There are numerous generally accepted and widely available frameworks for building a comprehensive information security program. These are either free or dirt cheap and they describe exactly how to build an information security program in any organization. A comprehensive approach is not expensive and there are not necessarily capital expenses involved.

You can use any of the following documents to begin building a comprehensive information and cybersecurity program.

ISO/IEC 27001[iv]

This is the international standard for building an information security program. It is available from the ANSI web store for $138. It is roughly 30 pages and describes exactly how to build a comprehensive security program for any organization from scratch.

NIST Framework for Improving Critical Infrastructure Cybersecurity[v]

This framework was created by NIST (The National Institute of Standards and Technology) and it is a risk-based approach to developing a cybersecurity program. It is available for free.

HIPAA Security Rule[vi]

The HIPAA Security Rule is a federal regulation (45 CFR parts 160, 162, 164) for protecting PHI, but it can also be used as a framework for building an information security program. If you have PHI (most counties do) to protect, you could start your program by building it on HIPAA and then use one of the other frameworks to supplement what HIPAA misses. A common misconception about HIPAA is that it is an onerous regulation that is difficult to comply with. In truth, HIPAA sets a low bar and you will definitely need to supplement a HIPAA compliance program with additional policies and procedures.

Action Plan - How to build a cybersecurity program – first steps

Building a comprehensive, standards-based cybersecurity program is a straightforward process. In general, we recommend an approach something like this:

1. **Establish a governance committee.**
   The membership of your governance committee should include people who are expert in various aspects of the information you maintain. For a county government, this might include the county recorder, corporate compliance, public or mental health, human resources, the county attorney, and information technology. A senior executive and a board member should also be on the committee.
2. **Get a risk assessment.**
   Risk assessment is an absolute requirement. If you have someone on the staff skilled in this, you can do it internally. If your organization has never gone through a risk assessment process, you should contract an outside firm for the first one unless you have staff members who are capable of objectively performing one. Risk assessments should be carefully scoped.
3. **Create an asset inventory**
   A complete, current inventory of all your information assets including digital data, applications, physical information (paper records), and hardware is an absolute requirement. Most local governments don't have this information in detail that would stand up to any kind of audit.
4. **Create a comprehensive security policy.**
   A primary responsibility of your governance committee will be to draft a comprehensive security policy that addresses your organization's unique needs relative to risk. The policy should be approved by your governing board. You can and should build your program on any of the three frameworks described above. You'll have to decide which one is the most appropriate depending on your unique business requirements.
5. **Create a risk management plan**
   The risk assessment process will identify many shortcomings in your information security program. It is the responsibility of your board and senior executives to identify risk appetite and priorities for risk mitigation.

How much work does it require?

Does all you have read so far sound straightforward and simple? It is.

There is no reason for any local government agency not to implement a comprehensive cybersecurity program. While the steps are simple, it may not be easy to implement and the problems you encounter are more likely to be administrative and procedural rather than technical. Technical implementation of a cybersecurity program is the easiest part; getting the management structure right is much more difficult.

If you proceed down the path to standards-based cybersecurity, you may find that it takes six months to a year to put all the policy and procedural components into place, get a risk assessment, make a plan, and implement it, but this all depends on the availability of resources and your commitment to the project.

How much does it cost?

Building a security program on standards and best practices may require no capital expenditures but it requires time and attention from managers throughout your organization. In general, local governments don't lack the funding for technical controls and many of them already have all the required technology in place. What local governments are generally missing are clear policies, procedures, and accountability.

Getting Help

If you would like assistance with your program, give us a call. We provide comprehensive management services for information security and can help you through every step of the process. Visit our website for more information on our services for local governments.

For a detailed multimedia overview of cybersecurity in local government, watch our video, Cybersecurity, risk, and liability in local government.

Ready to talk? Contact us!

Schedule a meeting e-mail us Call (607) 731-4097

Read my other publications

Information Security Articles

- How to use the NIST cybersecurity framework. *Security Magazine*, April 2018.
- Board and management responsibilities for information security. *CIO.com*, February 2018.
- 5 things J.S. Bach can teach you about information security. *CIO.com*, December 2017.
- Risk assessments for local governments and SMBs. *CIO.com*, May 2017.
- HIPAA as an umbrella for county/municipal cybersecurity. *CIO.com*, April 2017.
- County and municipal cybersecurity – Part 2. *CIO.com,* April 2017.
- County and municipal cybersecurity – Part 1. *CIO.com*, March 2017.
- May I see your comprehensive security policy please? *CIO.com*, October 2016.
- The ACA and the death of medical privacy. *CIO.com*, August 2016.
- Why should county commissioners and executives care about HIPAA? *Careers in Government*, February 2018.

Governance and Management Articles

- Information governance in the federal government. *CIO.com*, February 2018.
- Digital Transformation in the public sector. *CIO.com*, January 2018.
- Keep your dirty, stinkin' hands off my Internet. *CIO.com*, January 2018.
- For tech's sake! Another government tech plan? *CIO.com*, August 2017.
- What's new with ISO/IEC 20000? *CIO.com*, July 2017.
- How Nebraska successfully consolidated state IT services. *CIO.com*, June 2017.
- Municipal shared services agreements for information technology. *CIO.com*, May 2017.
- County/municipal IT services and the RACI model. *CIO.com*, May 2017.
- Information governance for counties and municipalities. *CIO.com,* April 2017.
- Is naked truth part of your business model? *CIO.com*, January 2017.
- Voodoo project management. *CIO.com*, January 2017.
- On the nature of "IT" projects. *CIO.com*, November 2016.
- Here's why your EHR doesn't work. *CIO.com*, November 2016.
- We can't afford quality! *CIO.com*, October 2016.
- High crimes and misdemeanors of CIO's. *CIO.com*, October 2016.
- What is the biggest threat to internal IT Departments? *CIO.com*, October 2016.
- Managing line-of-business projects. *CIO.com*, September 2016.
- Who should manage IT? *CIO.com*, July 2016.
- Is management a legitimate primary skill? *CIO.com*, July 2016.
- How to assemble a winning ERP team. *CIO.com*. June 2016
- How to survive an IT Management Audit. *CIO.com*. June 2016
- Management is everything. *Careers in Government,* April 2017.
- Accountability in the public sector. *Careers in Government,* October 2016.
- The high price of complaining. *Careers in Government,* July 2016.
- Fire your annual performance review. *Careers in Government,* June 2016.
- Municipal IT Director: 6 Must have qualities. *Careers in Government,* May 2016.

I hope you have found this information to be useful. Feel free to get in touch if you have questions or comments and I wish you the best of luck with your cybersecurity program.

Jeffrey Morgan
President
e-volve Enterprise Management Services
519 Blakeslee Road
Milan, PA 18831
(607) 731-4097
Jmorgan@e-volvellc.com

References

Following are links to resources we discussed in this document.

[i] 2018 Ponemon Institute Data Breach Study.

[ii] Top cybersecurity facts, figures and statistics for 2018.
[iii] One-third of data breaches led to people losing jobs.
[iv] ISO/IEC 27001
[v] NIST Framework for Improving Critical Infrastructure Cybersecurity
[vi] HIPAA Security Rule