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

Cybersecurity for Attorneys

A resource guide to information and cybersecurity practices for attorneys

Jeffrey Morgan
President, e-volve Enterprise Management Services

Reading Time – 15 minutes

e-volve

Contents

e-mail: jmorgan@e-volvellc.com

Why should attorneys be concerned about cybersecurity?

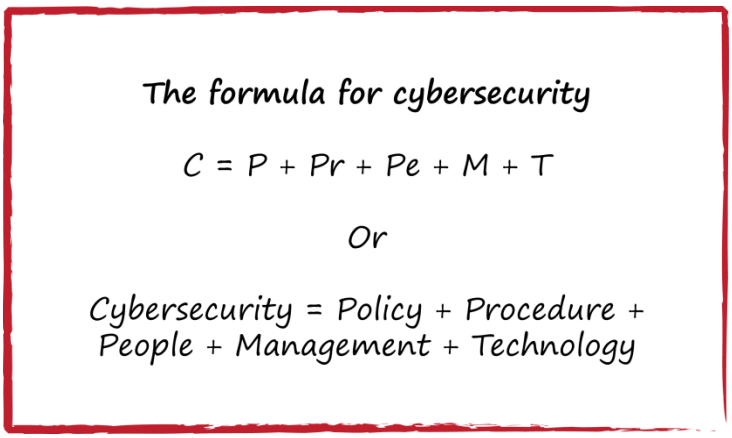
If your organization has a breach or other catastrophic information disaster, you'll be deeply involved in the aftermath and cleanup. It's what attorneys do. However, if you get involved before the disaster, you might be able to help prevent the disaster from occurring in the first place. If you are skeptical, keep reading.

In most organizations, especially in local governments, responsibility for cybersecurity has traditionally been turned over to Information Technology and it is entirely managed by an IT Director, CIO, or contractors and managed service providers. Typically, these IT-centric cyber and information security programs are ad hoc rather than comprehensive. **This is exactly the wrong approach** and it is not a practice advocated in any information security standard or framework.

According to a 2015 Ponemon Institute study, only 13 percent of local governments have mature cybersecurity programs. Attorneys can and should help solve this enormous problem by providing proactive guidance and leadership. Excellent cybersecurity programs are built on policy and procedure rather than on technology, so attorneys are a natural fit to participate in cybersecurity programs.

You might argue with me about this assertion. I get push back from non-security professionals all the time. "Jeff, attorneys have nothing to do with cybersecurity. Policy and procedure don't prevent cybersecurity incidents – technology does."

Nothing could be further from the truth. There are many moving parts to a good cybersecurity program and the formula for it looks something like this:



What fails in cybersecurity incidents and breaches?

Depending on what research you believe, 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.

e-mail: jmorgan@e-volvellc.com

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.

What most of these incidents and breaches have in common is that technology didn't fail – people failed. Policy and procedure 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.

Understanding Information Risk

Local government organizations bear enormous information risk but public sector boards and managers are rarely aware of just how much risk they are facing. County governments typically have vast quantities of PHI (Protected Health Information) and PII (Personally Identifiable Information). They rarely have programs in place that are sufficient to secure this statutorily protected information and most of these organizations are not even minimally in compliance with HIPAA and other state and federal regulations.

Many managers, executives, and board members may not see the need to worry about information risk. "What's the big deal? What can possibly happen?" Well . . . litigation, loss of reputation, loss of money (and lots of it), loss of business, and getting fired are some of the negative consequences of cybersecurity incidents. Attorneys tend see exactly what the big deal is more quickly than other members of the management team, especially if they have been trained in the relevant statutory requirements.

It is easy to identify whether your organization has implemented a standards-based cybersecurity program.

4 indications that your organization doesn't have a cybersecurity program

Risk assessment report

Can you lay your hands on a recent risk assessment report? Every information security standard, framework, and regulation requires formal, periodic risk assessments. If you don't have a risk assessment, you simply don't have a rigorous cybersecurity program.

Risk management program and plan

Your periodic risk assessment should be followed by documented processes and procedures to remediate the deficiencies discovered in the risk assessment. These activities should be formally reported to senior management and the governing body.

e-mail: jmorgan@e-volvellc.com

Top management and board oversight of information and cybersecurity

If senior managers, executives, and your governing board are not involved in oversight of your cybersecurity program, you don't have a rigorous program. The board should ask questions and it might be a good idea to have a board-level committee overseeing your cyber and information security programs. NACD (National Association of Corporate Directors) has an excellent document that defines questions boards should be asking about cybersecurity.

Comprehensive information security policy

A comprehensive information security policy for a complex organization such as a local government should be substantial - 25 pages or more. The HIPAA Security Rule requires a minimum of 40 policies and HIPAA actually sets a pretty low bar.

A good security policy is developed over a long period of time. In support of the policy, detailed procedures defining the processes and activities related to cybersecurity must also be extant. These documents along with evidence that the activities are conducted according to policy should be readily accessible and a clear chain of accountability and responsibility defined.

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 generally no capital expenses involved.

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

ISO/IEC 27001

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 from scratch.

NIST Framework for Improving Critical Infrastructure Cybersecurity

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

The HIPAA Security Rule is a federal regulation (45 CFR parts 160, 162, 164), but it describes a framework for building an information security program for an organization that maintains PHI. You could start your program by building it on HIPAA and then use one of the other frameworks to supplement what HIPAA misses.

e-mail: jmorgan@e-volvellc.com

Other regulations, guidelines, and policies

There are many state and federal regulations that govern information security for municipal government. CJIS (Criminal Justice Information Services) has a security policy for law enforcement agencies using its information products.

Depending on what state you are in, your state archivist, comptroller, attorney general, as well as additional agencies may also have guidelines for public sector organizations to follow. As the landscape of information security is constantly becoming more complex, public and private sector organizations are frequently failing to respond to new regulations and threats.

Building or improving your program

Municipal governments typically have all the resources they need already on staff to build excellent cyber and information security programs. However, the nature and complexity of information local governments manage is too complex to be overseen by a single CIO or IT Director unless they have extraordinary capabilities.

One of the first steps a local government should take is to establish an Information Governance committee to oversee the program and policy development. The composition of a good committee might include representation from the following departments:

- Governing Board
- Legal
- Human Resources
- Executive Management
- Records Management
- Information Technology
- Security
- Corporate Compliance
- Staff members who actually work with protected information
- Department managers who manage information (Public Health, Mental Health, Social Services, County Recorder, etc.)

I don't like to see these committees too top-heavy with senior management. Most top-down initiatives, at least in my experience, fail. A good information security program needs top-down, bottom-up, and inside-out management.

Action Items -

1. Establish a governance committee.
2. Catalog and prioritize your information assets so you know what you need to protect.
3. Get a risk assessment.

e-mail: jmorgan@e-volvellc.com

4. Develop a comprehensive security policy and get it approved by your governing board.
5. Define procedures, roles, and responsibilities.
6. Establish a remediation program to address deficiencies discovered in the risk assessment.
7. Improve your program with a cycle of continuous improvement.

This sounds simple, right?

It is. So, why isn't your organization doing it?

Summary

Standards-based information and cybersecurity programs are easy to setup and you have learned to quickly identify whether or not you have such a program in your organization. You have also learned how to build a cybersecurity program from scratch using a multidisciplinary team.

More Information

You may find my video, Cybersecurity, risk, and liability in local government to be of value and we have many additional resources on our website: http://e-volvellc.com. I wish you the best of luck with your Cybersecurity program and don't hesitate to contact me if you have questions.

Cybersecurity, cyber risk, and liability in local government

About Jeffrey Morgan

Jeffrey began his career in US Army Intelligence and has provided independent consulting services to local governments since 1993. He holds a Master of Arts from the University of California, Riverside and has experience in over a dozen business sectors including DoD, manufacturing, publishing, insurance, transportation, finance, retail, K12 education as well as federal and local government.

e-mail: jmorgan@e-volvellc.com

About e-volve Enterprise Management Services

e-volve Enterprises Management Services works with local governments and behavioral health organizations to improve quality and services, lower costs, and reduce risk. Feel free to e-mail or call me with any questions.

Jeffrey Morgan
President, e-volve Services
e-mail: jmorgan@e-volvellc.com
Phone: (607) 731-4097
Web: http://e-volvellc.com