CYBERSECURITY:

KEEPING OUT OF THE HEADLINES

by Anthony Munns

Cyberattacks and security breaches equal bad publicity and worse. As a municipality, you need to know the questions to ask your executive team to avoid hitting the headlines. Better yet, help identify the risks facing your organization and propose action steps to minimize those risks. Security and privacy is a continuous process, not just a product. Good compliance does not mean you are secure. It is crucial for all levels and departments within a municipality to be actively and continuously involved in awareness, prevention and responses to cyber security issues.

Vulnerability

With the number of large local, national and international companies that experienced data breaches in 2014 – Staples, Sony, Target, P.F. Chang's and The Home Depot – it's become harder to think any given company or municipality, for that matter, is immune. State and local government is not. Recently, John Byers, chief information security officer for the Kansas Department of Administration's Office of Information Technology Systems stated "the threats," sometimes include "socially engineered Trojans, phishing attacks, advanced persistent threats, network-traveling worms, just to name a few."

In 2013, 5.7 million current and former South Carolina taxpayers and their dependents had their personal information hacked from the department of revenue. Last month, after getting hacked by cyber activist group, Anonymous, for its homeless laws, the city of Fort Lauderdale updated its cyber security network with $430,000 worth of improvements. Closer to home, in December 2014, the Missouri State Employees Retirement System sent approximately 81,000 emails and 20,000 letters to members explaining that someone gained "unauthorized access" to four members' accounts and filled out online forms that required the use of the members' Social Security numbers, retirement ID numbers and passwords, and had shut the site down.

A study from Enigma Software found that in 2014, St. Louis experienced computer infections on a per capita rate that was almost 370 percent higher than the national average. *Forbes Magazine* recently reported that Patrick Morganelli, senior vice president of Technology at EnigmaSoftware.com, says that there isn't a particular reason for St. Louis and the other ranked cities to be experiencing higher rates of infection. Some factors have less to do with user behavior and more to do with network intrusions or malware piggy-backing on legitimate applications, he says.

The Cost Of Cybercrime

This comes on the heels of the Ponemon Institute's "2014 Cost of Cyber Crime Study" that found the average annual cost of cyber crimes is up 9.3 percent since last year, at $12.7 million per organization. Information theft amounts to 40 percent of total annual external costs for organizations, making it the highest external cost. An external cost is any cost created by external factors such as fines, litigation, marketability of stolen intellectual properties and others. Costs associated with business disruption or lost productivity are the second-highest external cost, accounting for 38 percent of external costs.

There is a positive association between the time it takes an organization to contain an attack and the organizational cost. The Ponemon study found that it takes an average of 45 days to resolve a cyber attack with an average cost of $35,647 per day. The total cost over the 45-day period, $1,593,627, represents a 33 percent increase from last year's cost estimate

that was based on a 32-day resolution period.

Organizations that deployed security intelligence systems enjoyed an average cost savings of $5.3 million and a return on investment (ROI) of 30 percent. To help reduce the risk of a cyberattack, organizations should first develop an information security policy, document it and disseminate it throughout the organization. Another protective measure is to develop an incident response plan to react to a breach and quarantine activity before it spreads throughout the organization's computer network.

The Expanding Threat

We traditionally consider the primary targets for cybercrime to be financial service institutions, but that is changing. If you analyze repeated incidents, the top five targets are universities, financial services, federal agencies, technology providers and hospitals, in that order. It is not just financial transactions that are being compromised; personal data, health information, and intellectual property are now sought.

The nature of the attackers is changing too. It is no longer just the techno geek in the wee hours; organized crime, nation states, and activist groups are moving in. The number of insider driven incidents is now more than 30 percent of reported incidents.

Information systems departments are aware of these disturbing trends, but continue to struggle with a lack of skilled information security resources. Even when they get management's support, there is a shortage of affordable qualified candidates.

Preventive Measures

The attack vectors are changing all the time, such as website hacking, spear-phishing, and skimming. Concentrating on perimeter defenses alone is insufficient. Security risk assessment, addressing internal vulnerabilities, security event information management (SEIM), and data leak prevention management are needed.

A comprehensive incident management plan that addresses mitigation, notification, and remediation is a must. An incident management plan is not just an IT department need, but a company need. Risk management, legal, and public relations all have roles. Executive management must be involved. A well-constructed plan helps you manage unexpected and disruptive events, minimize the impact and assist in maintaining or restoring normal operations within a defined time period. This is not an IT-only plan.

A key starting point for IT departments that want to seriously address these issues is to select an IT framework. A framework gives you an understanding of a comprehensive and integrated set of policies, procedures and controls, and helps minimize the risk that key areas are overlooked. There are many good frameworks available to consider:

- **COBIT 5 –** This is the leading framework for the governance and management of enterprise IT.
- **ISO 27001 –** The ISO 27000 family of standards helps organizations keep information assets secure.
- **ITIL –** The Information Technology Infrastructure Library (ITIL) defines the organizational structure and skill requirements of an information technology organization and a set of standard operational management procedures and practices to allow the organization to manage an IT operation and associated infrastructure.
- **NIST Cybersecurity Framework –** The National Institute of Standards and Technology framework has been recently announced and is under development. NIST released the first version of the Framework for Improving Critical Infrastructure Cybersecurity in February 2014.

To review frameworks in a side-by-side comparison, review the Cloud Security Alliance Cloud Controls Matrix Version 3.0.1. A quick online search will lead you to this service, available free of charge.

Finding Answers

What questions should you be asking your executive team? The following seven questions will help you develop your strategy to help your organization avoid being compromised:

- Do you perform an annual security risk assessment? Do you have a program to mitigate risks identified as they change?
- Do you have a security awareness program? Do you educate employees on how to handle confidential information, and what to do if they think there has been an incident?
- Do you harden, update and patch systems? Does this include all systems, programs and utilities?

- Do you use intrusion detection and data leak prevention? Do you monitor sensitive data and control it from leaving the organization?
- Do you utilize encryption? – Consider data at rest (hard drives, laptops, USB sticks, etc.); data in motion, such as sending files, email, texting; websites; peripherals, such as copy and fax machines, backup systems, etc.; and, all other places data may exist.
- Do you have a vendor management program? Have you determined if they are "fit for the purpose"?
- Do you have an incident response plan? Does it include all key partners: IT, forensics, legal, public relations, and management?

With increasingly complex environments – Internet, mobile, bring your own device (BYOD), cloud – going it alone is not an option for many organizations. For municipalities, the challenge of hiring experienced talent at an affordable cost is a challenge. Choosing an accredited, affordable cybersecurity partner wisely is a must.

Information security impacts all our lives on a daily basis. Due diligence and caution should be taken when divulging personal information via public networks and social media outlets. Security and privacy is a continuous process, not just a product. Having good compliance does not mean you are secure. Vulnerability assessment and penetration testing are two of the tools that can help an organization gain a better understanding of their security strengths and weaknesses.

Controls need to be defined, documented, and implemented to reduce the risk of information being viewed, accessed, or compromised. The proper mixture of people, processes, and technology needs to exist. Also, be sure your management and employees are educated on the risks and the necessary security precautions.

Cyber Insurance – Find The Right Coverage

Because cyberattacks can be just as damaging to an organization as a fire or other natural disaster, organizations should review their insurance options for cyber protection. Insurance policies cover things like the cost of fines, notification that personally identifiable information (PII) has been compromised, liability, and business interruption. Cyber policies vary, so organizations must be careful to buy the right coverage.

Stay On Top Of Developments

The need for information security will continue to increase as technology continues to evolve, becomes integrated into the mainstream of business processes, and once-defined perimeters continue to erode. It is important to keep up with this exploding crisis and the rapidly changing environment.

Information security impacts all our lives and we all have a role to understand and manage the risk. There are good tools out there to facilitate a comprehensive approach. Be a part of your organization's approach to manage and reduce that risk.❑

Tony Munns, FBCS, CITP, CISA, CIRM is the founding partner and leader of the IT Audit & Security practice at Brown Smith Wallace LLC. He speaks and writes extensively on IT audit, security, HIPAA and HITECH security matters, and helps many organizations from small to large manage the risks associated with the use of technology. Contact Brown Smith Wallace at (314) 983-1200 or info@bswllc.com.