Tips on implementing a cybersecurity program in your information agency

H. Frank Cervone, PhD, CPHIMS
Director of IT, CISO, and HIPAA Liaison
School of Public Health, University of Illinois at Chicago
Monday, October 17, Internet Librarian 2016
Cybersecurity is a concern for everyone

100% of retailers are worried about “privacy concerns related to security breach”

55% increase from 2011

http://www.itgovernanceusa.com/blog/100-of-retailers-worried-about-cybersecurity
Security of health care data is a major problem

Nearly 90% of healthcare organizations had some sort of data breach between 2013 and 2015

The estimated cost of this is over > $6.2 billion annually

Image courtesy of David Castillo Dominici at FreeDigitalPhotos.net

How to Do Whatever You Want on Library Computers

Three Methods:  ■ Use Firefox  ■ Get full functionality  ■ Create a Persistent USB drive  ■ Community Q&A

Many times, you are at the library and want to use some program, like Firefox, to browse the Internet. You might also want to take notes on something, but they won’t let you open anything! This is how to do that.

Method 1  Use Firefox

1 Get a USB flash drive. This will let you get your software onto the computer. If you plan to do heavy duty work from your USB drive, try to get at least a 1 GB drive.
Whale attacks

http://www.healthcareitnews.com/node/525131 - Image courtesy of the Washington Post
The problem is often inside

Pay up, and pay again

Lack of focus exaggerates the problem

http://www.itgovernance.co.uk/blog/54-of-boards-only-receive-cyber-security-updates-when-something-goes-wrong
90% of security problems can be solved simply

Have a meaningful security program

- Fear should not be the primary motivator
- Create a governance structure for security awareness
- Ensure you actually have meaningful security controls in place
- Focus on what to do, not what NOT to do
- Use diverse methods of training and awareness

Questions to get started

What are the types and sources of information in the organization?

What information is relied upon to make decisions?

Are there any types of information that should be kept more private than others?
Key things to address in developing a security policy

- **Scope**
  - People, systems, programs, information, facilities, networks

- **Management goals for secure handling of information**
  - Legal, regulatory, and contractual obligations

- **Relationship of policy to other directives and supplementary documents**

- **Information classification**
  - Content-specific definitions

- **References to supporting documents**
  - Roles and responsibilities, process, technology standards, procedures, guidelines

- **Specific instruction**
  - Organization-wide security mandates
  - Specific designation of responsibilities

- **Consequences for non-compliance**
Sample policies

https://www.sans.org/security-resources/policies
Keys topics in a security awareness program

- Security risks to the organization
- Creating and securing passwords/authentication
- Social engineering risks
- Virus and intrusion attacks
- E-mail and Internet security exposures
- Securing desktops, laptops, and mobile devices
- Physical access to buildings and networks
- Policies related to data security and privacy
- Business continuity
- Regulatory compliance
- Who to contact
Free tech training

http://www.cyberaces.org/courses/

https://www.cybrary.it/
Some first steps

Start with HR and the hiring process

Enabling logging for all online transactions

Audit all program code put into production

Security awareness training for all employees

Implement account management policies and practices
  • Consider time-based access

Enforce separation of duties and computing with least privilege
  • Enforce use of privileged accounts only for administration

Regular organization-wide risk assessment (IT and non-IT)
Thank you

Frank Cervone, PhD, CPHIMS
Director of Information Technology and College
Information Security Officer
School of Public Health
University of Illinois at Chicago
fcervone@uic.edu