

Largest Risk for Public Pension Plans (Other Than Funding) – Cybersecurity

2017 Public Safety Employees Pension & Benefits Conference

Ronald A. King
(517) 318-3015
rking@clarkhill.com

CLARK HILL

“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Former FBI Director Robert Mueller
RSA Cybersecurity Conference
March 2012

2017:

Equifax: 143 million accounts affected

X-Box: 1.2 million accounts affected

2016:

Yahoo!: 500 million accounts stolen (“state-sponsored actor” allegedly responsible)

Verizon Enterprise Solutions: 1.5 million accounts affected

2013:

Target: 40 million credit and debit card accounts taken (\$252 mil cost/\$90 mil covered)

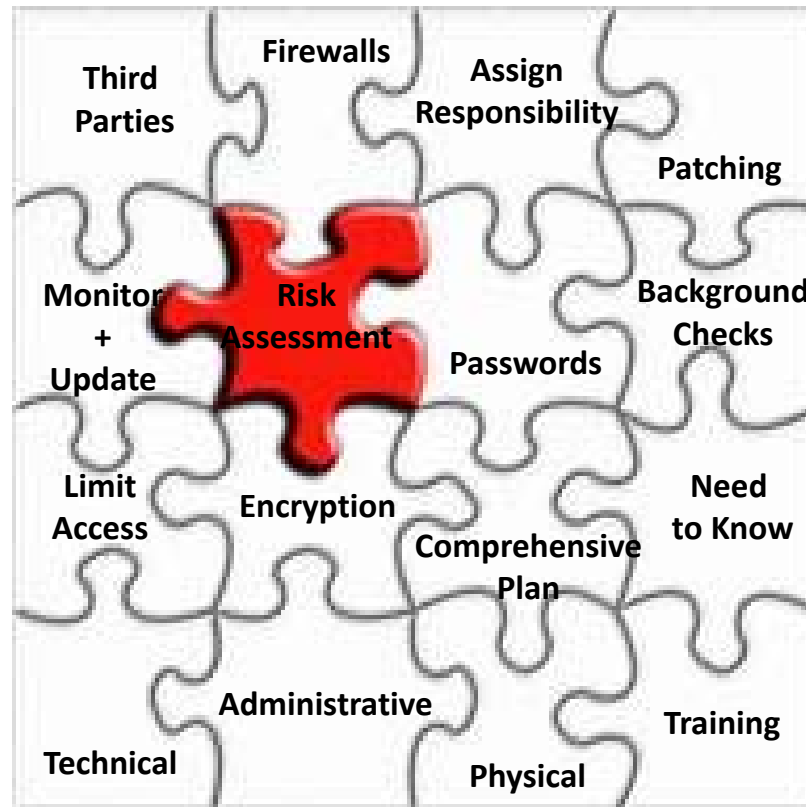
IF A BREACH OCCURS, EXPECT LITIGATION (LIKELY CLASS ACTION)

THREAT ACTORS

- Cybercriminals
- Hackers
- Hactivists
- Government surveillance
- State sponsored / condoned espionage
- Insiders (disgruntled/dishonest/bored/untrained)



SECURITY REQUIREMENTS



KEY SECURITY QUESTIONS

- Have you performed a risk assessment?
- Do you have an actionable incident response plan?
- What tools do you have to manage situations/consequences?
- Do your processes allow for effective management in crisis?
- Have you identified key personnel in the event of a crisis?
- Have you trained your employees lately on cybersecurity?
- Have you updated your privacy policy?
- Do you have a recent terms & conditions on your site?
- Would you consider yourself security aware?

If you answered “NO” to any of these, why is that?

INCIDENT RESPONSE PLANS

Preparing for **WHEN** a business will be breached,
not **IF** your organization may be breached

Words to Live by:

Identify & Protect + **Detect, Respond & Recover**

PUBLIC PENSION SYSTEMS

Personally Identifiable Information (“PII”) to consider:


- Social Security Numbers
- Dates of Birth
- Addresses
- Bank Account Information
- Protected Health Care Information (administration of disability benefits)

PUBLIC PENSION SYSTEMS (CONT.)


Unique Challenges

- Antiquated IT systems
- Reliance on plan sponsors data management systems
- Limited resources
- Trustee buy-in
- Recruiting, attracting and retaining qualified staff

CYBERSECURITY ASSESSMENTS


CBI
IT Risk Management

External Vulnerability Assessment


RSCD
Retirement System City of Detroit

Prepared by:
Reid Brosko / CISSP
rbrosko@cbitime.com

800.747.8585
June 5th, 2015
Version 2.0
Page | 1

CBI
1260 Woodward Heights
Ferndale, MI 48220
<http://cbitime.com>
800.747.8585

CYBERSECURITY INSURANCE

Even with an incident response plan and cybersecurity tools in place, you should still consider cybersecurity insurance as a fail safe to protect your business from cyber risks

- Standalone coverage usually
- Helps companies recover faster from data loss owing to a security breach or other cyber event
- Transfers some of financial risk of security breach
- Investigate current coverage before you apply
- Know the limitations of your coverage (likely will not cover theft of intellectual property)

TYPES OF INSURANCE

- Data breach/ privacy crisis management
- Multimedia/ Media liability coverage
- Extortion liability coverage
- Network security liability

INSURANCE CONSIDERATIONS

- Security controls to reduce premiums
- Undertaking a security risk review
- Assistance to improve information governance and information security
- Malicious act by employees
- Uncertainty about breaches prior to coverage
- Media protection
- Response plans/ roles of outside professionals
- Litigation/ Defense costs
- Choosing a broker

CYBER LIABILITY PROGRAM (1/2)

- NCPERS has partnered with Ullico and Arthur J. Gallagher & Co. to create a proprietary Cyber Liability policy with preferred rates and a simplified 5-question application process. The program is designed to provide limits ranging from \$250,000 to \$2MM with higher limits available upon request and a broad range of deductibles beginning as low as \$2,500.
- Coverage includes:
 - **Privacy liability.** Losses arising from failure to protect sensitive personal or health information in electronic or hard copy format. Includes regulatory defense and settlement
 - **Breach Notification.** Data Breach counsel to provide immediate triage and consultation. Data Breach network of experts providing crisis management services including legal, computer forensics, regulatory and individual notification guidance, call center, credit monitoring and identity restoration services.
 - **Multimedia Liability.** Coverage for claims related to multimedia activities such as defamation, libel, plagiarism or copyright infringement.

CYBER LIABILITY PROGRAM (2/2)

- Coverage includes (cont.):
 - **System Damage.** Restore, re-collect, and replace data. Hire specialists, investigators, forensic auditors, and loss adjusters to review to substantiate the loss.
 - **Business Interruption.** Net income policyholder would have earned. Loss of Business Income including normal operating expenses that were incurred or affected by the event.
 - **Regulatory Actions.** Coverage for civil regulatory actions, expenses related to information requests, compensatory awards, and regulatory penalties and fines to the extent permitted by law.
 - **Cyber Threats & Extortions.** Monies paid by policyholder following threat.
 - **PCI Fines.** Fines and penalties from non-compliance with Payment Card Industry Data Security Standards.

QUESTIONS?



Ronald A. King

(517) 318-3015

rking@clarkhill.com

THANK YOU

Legal Disclaimer: This document is not intended to give legal advice. It is comprised of general information. Persons facing specific issues should seek the assistance of an attorney.

CLARK HILL