Does Your Firm Need Cyber Insurance?

DPLE 286
RLI Design Professionals is a Registered Provider with The American Institute of Architects Continuing Education Systems. Credit earned on completion of this program will be reported to CES Records for AIA members. Certificates of Completion for non-AIA members are available on request.

This program is registered with the AIA/CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing, or dealing in any material or product. Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.
According to the FBI’s Internet Crime Complaint Center, nearly 300,000 internet crimes were reported in 2016, totaling over $1.4 billion in losses. In 2015, cyber crimes cost the world more than $3 trillion and are expected to exceed $6 trillion in costs by 2021.

This course will explore risks to professional service firms, costs associated with certain types of internet crimes, benefits of the insurance designed to cover those risks, and other non-insurance protections.
Learning Objectives

Participants in this session will:

- Review some of the cyber risks faced by a typical design firm.
- Evaluate the costs associated with those risks.
- Consider benefits included with various insurance options.
- Examine other forms of cyber risk management.
The Risks
Hacking involves an alteration to computer software that allows the hacker to gain access to a firm’s administrative controls.

Hackers have outstanding programming skills and a deep understanding of the systematic workings of a computer.
Think ransomware is going away?

Think again...
Cloud Computing

2016 report by QuickBooks

Percentage of businesses using cloud computing:
• 2014: 27%
• 2016: 62%

By 2020, Forbes estimates that the global cloud IT market will reach $390B in revenue:
• Reduces cost and complexity
• Streamlines customer service
• Enhances collaboration opportunities
• Increases security
Cloud Vulnerability

Gartner predicts that 95% of all security issues and cloud failures will be attributed to user error by the year 2020.
Social Engineering manipulates people into divulging information or performing action. Social Engineering does not involve breaking into the computer system.
Social Engineering Techniques

Pretexting
- Obtaining personal information under false pretenses through surveys, phone calls, etc.

Phishing
- Gathering personal information through links that appear legitimate.
- Using a sense of urgency to manipulate a user into acting promptly.

Baiting
- Promising a good or service to entice a victim.
  - Free software downloads after providing login credentials
  - Distributing USBs infected with a virus.

Tailgating
- Impersonating an employee and going into restricted areas to gain information
How Does Social Engineering Work?

Individuals targeted over the phone or online

Criminals pose as a trusted coworker or employee of a company (i.e. bank)

Criminals exploit weakest link (human being) into divulging valuable info or wiring money
Loss or Theft of Devices

33% of Android users don’t use a lockscreen

33% of smartphones are broken or lost

According to a 2016 survey of CIOs, device theft occurs:

- 25% in cars and transportation
- 23% from the office
- 15% in airports and hotels
- 12% from restaurants
Confidentiality Breaches

Design Professional shall treat as confidential and not disclose to any third parties, except as necessary for the performance of this Agreement or as required by law, or use for its own benefit, any of Owner’s confidential information, know-how, discoveries, production methods and the like that is so identified in writing and disclosed to Design Professional or which Design Professional acquires in performing the Services required by this Agreement. Owner and Design Professional shall each specify those items to be treated as confidential and shall mark them as “Confidential.”

-ConsensusDOCS 240, Revised 2017
The Costs
90% of attacks come in the form of an e-mail

$5.3 Billion total losses between October 2013- December 2015 due to business e-mail compromise scams

2,370% increase in Identified Expected Losses between January 2015 – December 2016

40 Million e-mails passed through e-mail security

- 9 million pieces of spam
- 8,318 dangerous file types
- 1,669 known, 487 unknown malware attachments
- 8,605 impersonation attacks
What Makes Breaches Expensive?

Legal fees

Investigation costs

Client notification expenses

Credit/identity monitoring costs

Data restoration expenses

Down time
Types of Claims

- Failure to protect claimant’s information
- Reduction in value of claimant’s information
- Failure to timely notify of a breach
- Costs to remedy:
  - Credit monitoring
  - Identity theft insurance
  - Fines and penalties
- Fraudulent activity
- Damaged IT equipment
  - Inspection
  - Repair
  - Replacement
The Benefits
Types of Insurance

- Property coverage
- Privacy protection coverage
- Other coverages
  - Professional liability
Services

- Breach response
- Forensics
- Breach notification
- Credit monitoring
Other Forms of Cyber Risk Management
Everyone Forgets the Basics

1. Establish and maintain policies
2. Install firewalls
3. Mandate strong passwords
4. Update passwords frequently
Everyone Forgets the Basics

- Use anti-virus software
- Maintain systems and applications
- Restrict data access
- Limit server access
Everyone Forgets the Basics

- Create unique user ids
- Two-step sign-ins
- Track and monitor usage
- Encrypt vulnerable data
- Enforce protections
Everyone Forgets the Basics

- Don’t click on links or attachments
- Verify wire transfers by phone
- Run security checks
- Know signs of secure sites
- BACKUP DATA
Cloud Access Security Brokers (CASB)

CASB programs offer unique abilities to collect usage data from system users.

Data can be used to evaluate cyber exposures.

CASBs also provide value by integrating with existing security solutions, allowing for a uniform set of security and compliance policies across on-premise and cloud environments.
Don’t Feed the PHISH

If you’re contacted unexpectedly:

from someone asking you to confirm personal information such as an account number, password, or PIN...

About a warning that your account will be shut down unless you “reconfirm” your info...

By a “prospective employer” asking for personal information...

CALL the company or financial institution to see if the e-mail is legitimate
Thank you for your time!

QUESTIONS??

This concludes The American Institute of Architects
Continuing Education Systems Program

Alayne McDonald, Professional Development Coordinator
Alayne.McDonald@rlicorp.com
Vince Costello, Director of Underwriting
Vince.Costello@rlicorp.com
Laura Malloy, Underwriting Manager
Laura.Malloy@rlicorp.com
Clarence Sproul, Underwriter
Clarence.Sproul@rlicorp.com