RLI®

DIFFERENT WORKS

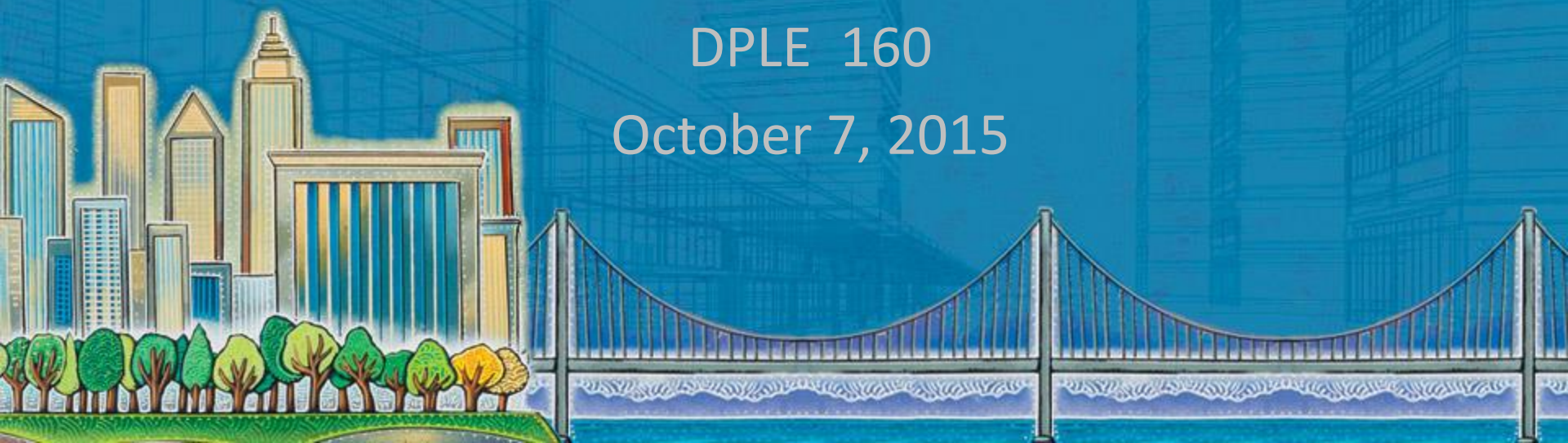
Cybersecurity: A Growing Concern for All Businesses

RLI Design Professionals

Design Professionals Learning Event

DPLE 160

October 7, 2015



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.

Copyright Materials

RLI®

DIFFERENT WORKS

Course Description

Hackers are increasingly becoming more sophisticated. **Phishing** schemes are on the rise and **ransomware** is one of the newest threats to all businesses. There is a **cost** to every cyber-attack whether it's **money, data, and/or loss of time and resources**. Join us for this cybersecurity update and learn more about what threats are out there lurking around your business waiting to attack your vulnerability. We'll also discuss **best practices** that you may consider in addressing your business's cyber security issues.

Learning Objectives

Participants will:

- Identify and define key cybersecurity threats to businesses of all sizes;
- Explore specific examples of real cybersecurity threats;
- Learn about best practices in addressing cyber security issues; and
- Understand where businesses can find credible resources to protect their business.

Brief Overview

What

- Malware
- Phishing
- Social Engineering
- Malicious Spam

Who

- Hackers
- Thieves

Point of Entry

- Employees
- Mobile Technologies
- Weak Passwords
- Vendors

Privacy Breach

- **Notification costs**
- **Credit monitoring**
- **Call center services**
- Forensics
- Crisis response
- Legal fees
- Defense costs and settlement expenses
- Regulatory fines and/or assessments

Privacy Breach Statistics

- **Humans** caused 53% of losses
  - **Hackers** caused 31% of incidents
  - **Insider involvement** in 32% of incidents
  - **Third parties** accounted for 25% of incidents
- Information targeted – **Personally Identifiable Information (PII)** most frequently exposed

- **$964.31** - average cost per record
- **$499,719** – average cost of crisis services
  - forensic,
  - notification, and
  - legal guidance etc.
- **$434,354** – average cost of legal defense
- **$880,839** – average cost of legal settlement

NetDiligence® 2015 Cyber Claims Study

Malware Defined

Malware is **mal**icious soft**ware** that works to take full control of a victim's computer and encrypt all files that are stored on the machine, rendering it unusable and inaccessible without the encryption key.

Includes:

- Computer viruses
- Worms
- Trojan horses

Is This Email Legitimate?

Wed 6/17/2015 2:01 PM

Reid, Colman <ReidC@wpunj.edu>

RE: EMAIL ANNOUNCEMENT!!

To Reid, Colman

Retention Policy RLI - Default - All Content - 7 Year Delete (7 years) Expires 6/15/2022

Take note of this important update that our new web mail has been improved with a new messaging system from Owa/outlook which also include faster usage on email, shared calendar,web-documents and the new 2015 anti-spam version. Please use the link below to complete your update for our new Owa/outlook improved web mail.

CLICK HERE TO UPDATE

Connected to Microsoft Exchange

Phishing Example

Unknown company or email address

Wed 6/17/2015 2:01 PM

Reid, Colman <ReidC@wpunj.edu>

RE: EMAIL ANNOUNCEMENT!!

To Reid, Colman

Retention Policy RLI - Default - All Content - 7 Year Delete (7 years) Expires 6/15/2022

Grammar errors

Take note of this important update that our new web mail has been improved with a new messaging system from Owa/outlook which also include faster usage on email, shared calendar,web-documents and the new 2015 anti-spam version. Please use the link below to complete your update for our new Owa/outlook improved web mail.

Links in email

CLICK HERE TO UPDATE

Popular Company

Connected to Microsoft Exchange

Red Flags in Phishing Emails

- Spelling errors
- Grammar errors
- Links in email
- Threats
- Spoofing popular websites or companies
- Using web addresses similar to well-known companies

Red Flags in Phishing Emails

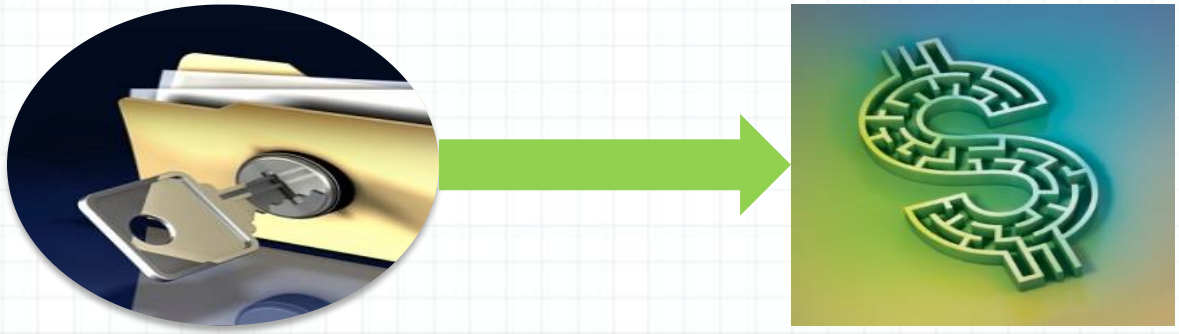
Solution – Think Before You Click

Ask yourself….

- Do I know the person that sent me the email?
- Is there a reason why they would send this to me?
- Does the message have a general greeting?
- Does the message ask me to do something (like login to an account, or open an attachment)?

Ransomware Defined

Ransomware is a form of **malicious software** that locks and restricts access to the infected computer. The malicious software will then display a message that **demands a ransom or payment** to remove the restriction.



Ransomware - Some Statistics

- Ransomware attacks more than doubled in 2014, from 4.1 million in 2013, to 8.8 million
- File-encrypting ransomware ("crypto-ransomware") grew from 8,274 in 2013 to 373,342 in 2014

Symantec Internet Security Threat Report, April 2015

Crypto-Ransomware

As a threat, Crypto-Ransomware grew exponentially at 45 times greater in 2014 over 2013:

- Cryptolocker
- Cryptodefense
- Cryptowall

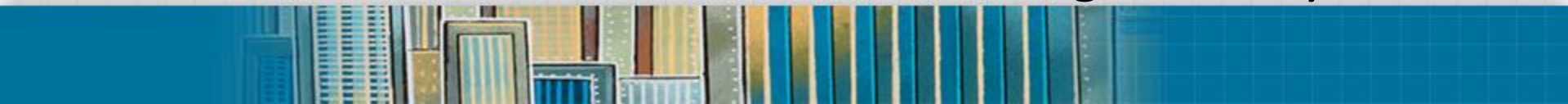
Cryptolocker Claim

Scenario:

- Cryptolocker virus detected by IT
- Request for employee to shut down system – occurred within 10 minutes of detection
- IT confiscated laptop
- Employee had no access to files on hard drive

Outcome:

- 4 days to recover files from hard drive
- Costs?
  - 4 days of reduced productivity
  - Time and expense for IT department to recover data
  - Loss of IT resources during recovery



Social Engineering Defined

Social Engineering means (in the context of security) the art of manipulating people to divulge confidential information.

- e-commerce involving targeting servers and backend databases
- Malware is hosted on web servers and distributed by phishing attacks or “drive-by” downloads

Point of Entry: Employees

Studies show that 30% of data breaches result from **human error** or **negligence**

Point of Entry: Mobile Technologies

100% of mobile applications tested by Trustwave for their 2014 Global Security Report had **at least 1 vulnerability**

Point of Entry: Weak Passwords

Weak passwords contributed to **31% of compromises** investigated by Trustwave for their 2014 Global Security Report

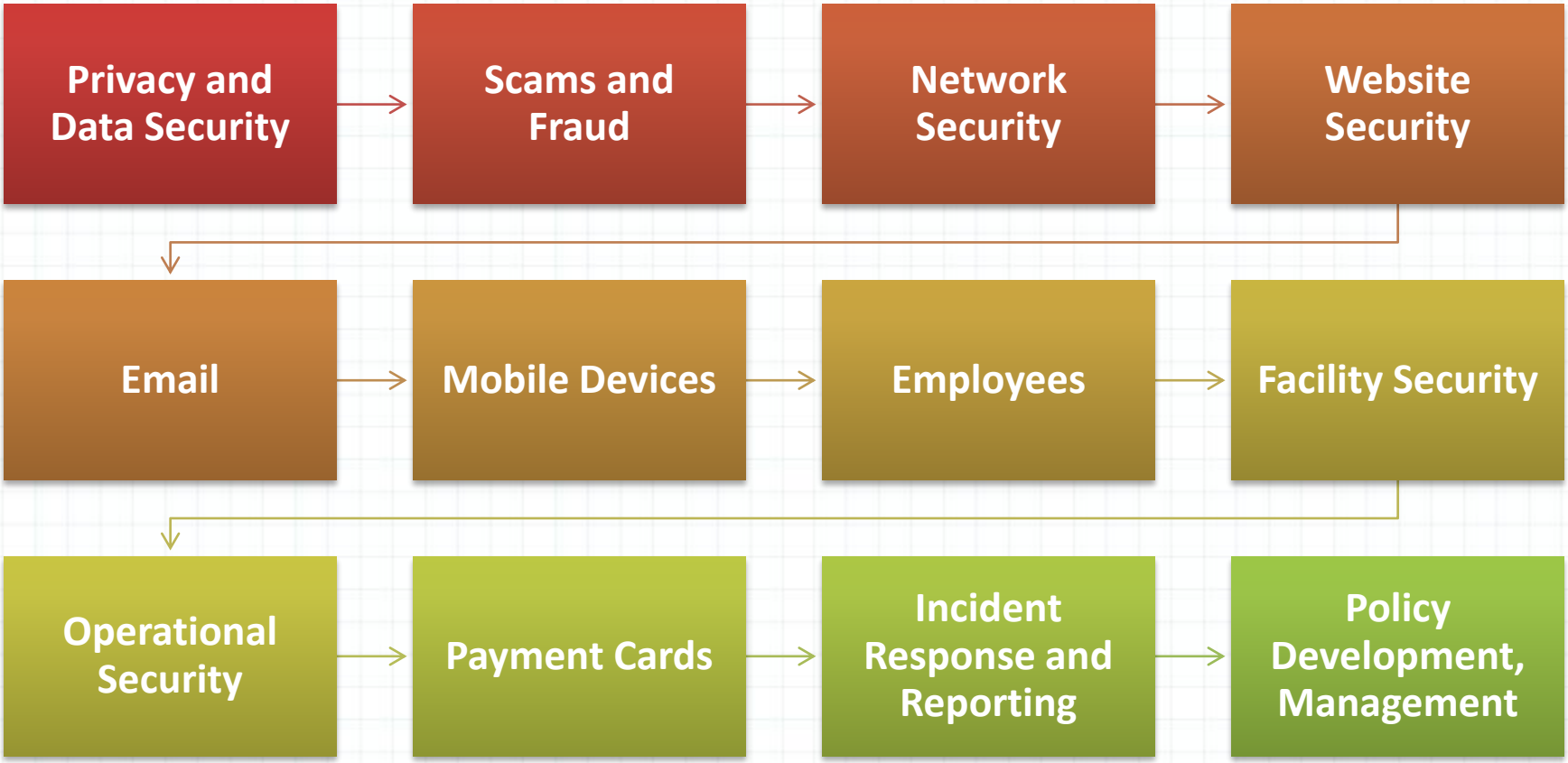
Point of Entry: Vendors

In 46% of incident response investigations, a major component of IT support was outsourced to a third party responsible for system support

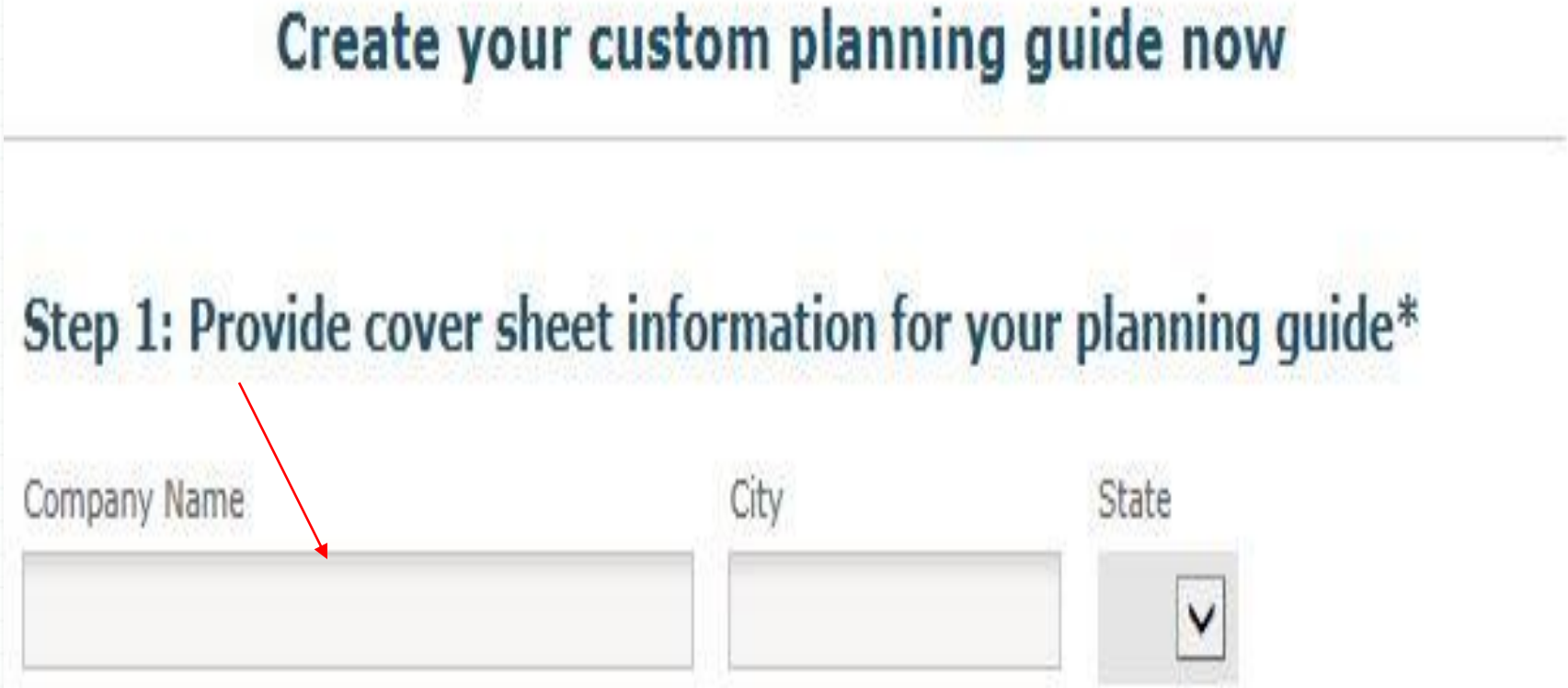
Trustwave 2014 Global Security Report

Resources

Federal Communications Commission – Small Biz Cyber Planner 2.0



Snapshot: Federal Communications Commission – Small Biz Cyber Planner 2.0



Snapshot: Federal Communications Commission – Small Biz Cyber Planner 2.0

Snapshot: Federal Communications Commission – Small Biz Cyber Planner 2.0

Step 3: Click below to finish

GENERATE YOUR PLAN

Or click here to download all sections of guidance.

Don't forget to consult with a qualified cyber security professional

This guide is not a substitute for consulting trained cyber security professionals.

Snapshot: Federal Communications Commission – Small Biz Cyber Planner 2.0

Email

Email has become a critical part of our everyday business, from internal management to direct customer support. The benefits associated with email as a primary business tool far outweigh the negatives. However, businesses must be mindful that a successful email platform starts with basic principles of email security to ensure the privacy and protection of customer and business information.

Cyber Plan Action Items:

1. Set up a spam email filter

It has been well documented that spam, phishing attempts and otherwise unsolicited and unwelcome email often accounts for more than 60 percent of all email that an individual or business receives. Email is the primary method for spreading viruses and malware and it is one of the easiest to defend against. Consider using email-filtering services that your email service, hosting provider or other cloud providers offer. A local email filter application is also an important component of a solid antivirus strategy. Ensure that automatic updates are enabled on your email application, email filter and anti-virus programs. Ensure that filters are reviewed regularly so that important email and/or domains are not blocked in error.

Excerpt from the FCC Small Biz Cyber Planner 2.0

Snapshot: Federal Communications Commission – Small Biz Cyber Planner 2.0

Definition Section

Phishing

Soliciting private information from customers or members of a business, bank or other organization in an attempt to fool them into divulging confidential personal and financial information. People are lured into sharing user names, passwords, account information or credit card numbers, usually by an official-looking message in an email or a pop-up advertisement that urges them to act immediately, usually by clicking on a link provided. See also **Vishing**.

Definition excerpt from the FCC Small Biz Cyber Planner 2.0

Resources

Federal Trade Commission- The Red Flags Rule

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations.

https://www.ftc.gov

Resources

- *www.fcc.gov*
- *www.ftc.gov*
- *A cybersecurity professional*
- *Legal counsel*
- *Your broker*
- *Your insurance company*

Thank you for your time!

QUESTIONS??

This concludes The American Institute of Architects Continuing Education Systems Program

Laurel Tenuto, Client Risk Management Coordinator
Laurel.Tenuto@rlicorp.com

Marie Bernier, Senior Risk Management Consultant

Marie.Bernier@rlicorp.com

RLI® DIFFERENT WORKS