RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

Cybercrime and Cyber Insurance Basics

**Presenters: Eric Himes &
Brian Thompson**

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

Disclaimer

This program or presentation is only a tool to assist you in managing your responsibility to maintain safe premises, operations and equipment and is not for the benefit of any other party. The program or presentation does not cover all possible hazardous conditions or unsafe acts that may exist, and does not constitute legal advice. For decisions regarding use of the practices suggested by this program or presentation, follow the advice of your own legal counsel. Resource Partners disclaims all forms of warranties whatsoever, without limitation. Implementation of any practices suggested by this program or presentation is at your sole discretion, and Resource Partners or its affiliates shall not be liable to any other party for any damages whatsoever arising out of, or in connection with, the information provided or its use. This material does not amend, or otherwise affect, the provisions or coverages of any insurance policy or bond, nor is it a representation that coverage does or does not exist for any particular claim or loss under any such policy or bind. Coverage depends on the facts and circumstances involved in the claim or loss, all applicable policy or bind provisions, and any applicable law.

For every lock, there is someone out there trying to pick it or break in.

- David Bernstein

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

Today's Agenda

- Latest Stats
- Common Terms
- Claim Examples
- Risk Management
- I've experienced a breach! Now what?
- What is Cyber Insurance?
- Questions

Well Known Attacks

Target – 40M credit card credentials; 70M customer records

Marriott International – 500M consumers

Yahoo – 3B users

Average cost of a data breach in 2020 is $3.86M*

***per IBM and Ponemon Institute**

Common Terms

Ransomware – malicious software that prevents users from accessing their systems or data until ransom is paid

Internet of Things (IOT)– the interconnection of embedded computing devices in everyday objects, enabling them to send or receive data

Phishing – scheme to acquire private personal or financial information using fraudulent e-mail message

Common Terms

Social Engineering – use of deception to manipulate individuals into divulging confidential or personal information to be used for fraudulent purposes

Reverse Social Engineering – special form of social engineering where the victim unwittingly seeks help from the attacker.

Denial of Service (DOS) Attack – flooding network with traffic to prevent legitimate users from accessing the network

Common Terms

Cryptojacking – unauthorized use of someone else's computer resources to mine cryptocurrency.

Dark Web – virtual marketplace where criminals can buy/sell/trade stolen information, purchase computer viruses and obtain other illegal products

Botnet – collection of compromised computers under the control of another entity. These computers are used to complete DOS attacks, Cryptomining or other nefarious attacks.

Common Terms

PII

Personally Identifiable Information

- Social security and driver’s license numbers
- Bank account information
- Online account user names and passwords
- Health insurance information.

PHI

Protected Health Information

Information relating to the provision and payment of health care that can be used to identify an individual.

PCI

Payment Card Information

Debit and credit cards

Breach Expenses

2020 average cost per record breached:

$242 (Up almost 50% in 5 years)

*Data compiled by Ponemon Institute Research Report 2020

Recent Claims

Date Made Public:
October 2, 2017
Company: Arkansas Oral Facial Surgery
Location: Fayetteville, Arkansas
Type of breach:
HACK
Type of organization:
MED
Records Breached:
128,000
Total Records:
128,000
"A ransomware attack on Fayetteville-based Arkansas Oral Facial Surgery Center has potentially breached the data of 128,000 of its patients.
An investigation found the cyber attack occurred between July 25 and 26, and while quickly detected, the virus encrypted x-ray images, files and documents. Fortunately, the patient database was not encrypted.
However, hackers managed to infect the data of a small number of patients who visited the provider within three weeks prior to the incident."

Information Source:
http://www.healthcareitnews.com/news/ransomware-attack-breaches-128000-patient-r...

Recent Claims Continued…

Date Made Public:
August 31, 2017
Company: McLaren Medical Group (MMG)
Type of breach:
HACK
Type of organization:
MED
Records Breached:
106,008
Total Records:
106,008

In March of 2017, Michigan-based McLaren Medical Group (MMG) learned its computer system had been accessed by an unauthorized party, leading to a health data breach, according to an MMG statement issued to *HealthITSecurity.com*.

The accessed system stored scanned documents including information related to authorizations, orders, appointment scheduling, and similar data. The breach occurred at MMG's Mid-Michigan Physicians P.C. practice.

Scanned documents may have included patient information such as patient names, dates of birth, addresses, phone numbers, medical record numbers, diagnoses, and Social Security numbers.

Information Source:
https://healthitsecurity.com/news/mi-computer-system-health-data-breach-may-invo…

Risk Management Strategies

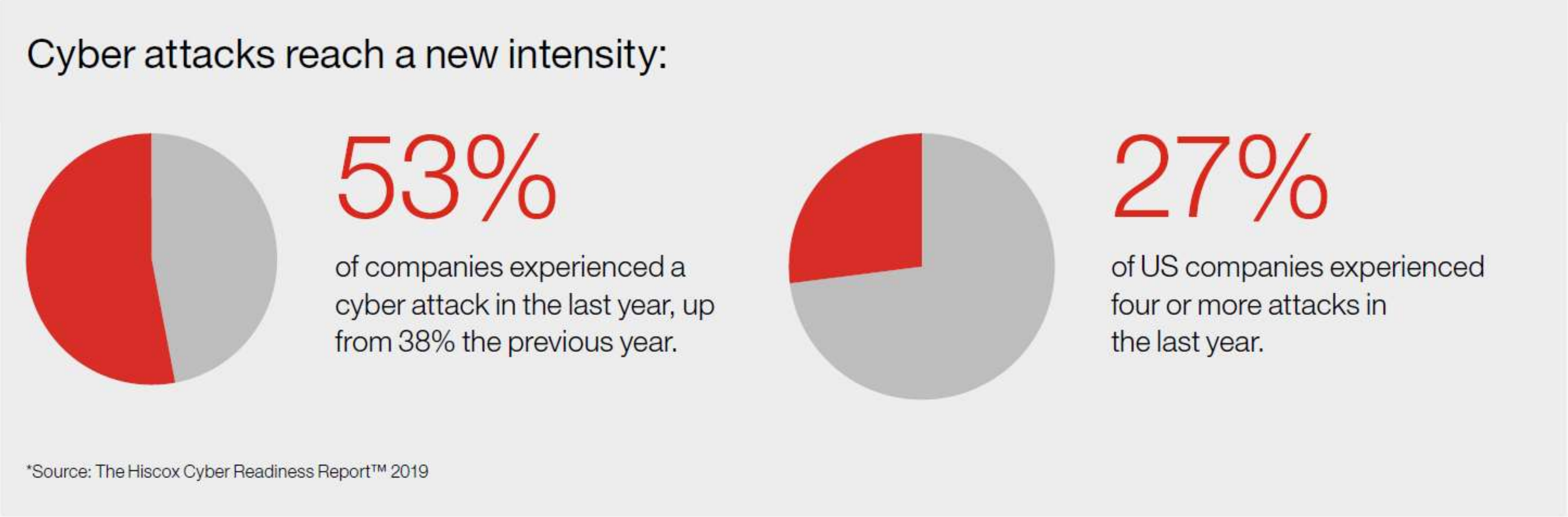
An **ENTERPRISE RISK MANAGEMENT** approach to *privacy security* is necessary to mitigate the risk of a data breach and decrease the damage when a breach occurs.

This **STRATEGIC** approach to *data breach prevention* and response involves a combination of best practices, insurance and a response plan.

Risk Management Strategies

The COVID Impact

- 64% of Americans are now working from home on at least a part-time basis*



Cyber attacks reach a new intensity:

53%

of companies experienced a cyber attack in the last year, up from 38% the previous year.

27%

of US companies experienced four or more attacks in the last year.

*Source: The Hiscox Cyber Readiness Report™ 2019

Pre-Incident Prevention

- Invest in a Virtual Private Network (VPN)
- Make privacy & data security part of the corporate culture by:
  - Knowing what data you have where
  - Increase employee training with periodic testing
    - Be cautious with emails
    - Strong Passwords (or Passphrase)
    - Consider Multi-Factor Authentication (MFA)
  - Keep computer systems updated

Pre-Incident Prevention

- Be proactive
  - Have detailed risk mitigation plans and disaster recover plans
  - Test your plans regularly
  - Regularly Review & Update existing plans & policies
  - Document your preparations
- Assign ultimate data privacy and security responsibility to one person but work & plan together
- Understand the significance of what a loss could mean

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

Pre-Incident Prevention

- Assess Relationship with Vendors and Business Associates
- Collect and retain the minimum of personal information necessary
  - Respect the rights of Data subjects
    - Ensure consent is understood to be freely given by data subjects
    - Evaluate and update your Privacy Statement
- Mitigate Risk & Expense with Security and Privacy Insurance.

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

I’ve experienced a breach!

Cyber Risk Incident Response

- Forensic Investigation
  - Determine what happened
  - What information was lost, damaged or stolen
  - Are we still vulnerable to attack?
- Who needs to be Notified
  - Government
  - Individuals
  - Media (Public Relations)
- Prevention and Mitigation
  - How do we better prepare for the next time

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

I’ve experienced a breach!

Cyber Risk Incident Response

- Invest in the services of a Breach Coach to assist with
  - Required notifications
  - Retain forensic professionals
  - Crisis communications

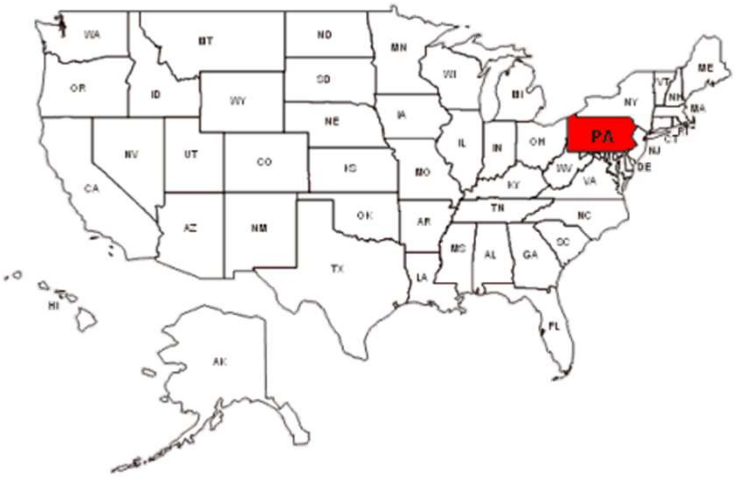
RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

State Regulations

Each State has criteria as to when an individual must be notified after a breach

FIRST NAME/INITIAL & LAST NAME PLUS ONE OF THE FOLLOWING:

- Social Security number
- Driver's license or state
- Identification card number
- Financial account
- Credit card or debit card number in combination with any required security or access code or password that would permit access to a resident's financial account.



RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

What is Cyber Insurance

- Cyber Risk is commonly defined as exposure to harm or loss resulting from breaches of or attacks on information systems. This can be related to activity online via the internet including your electronic systems and technology network.

What does it cover?

- Human Error
- Virus Transmission
- Employee Sabotage
- Data Breach
- Cyber Extortion

What is Cyber Insurance

Data Breach Definition
Unauthorized access and acquisition of unencrypted and un-redacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident

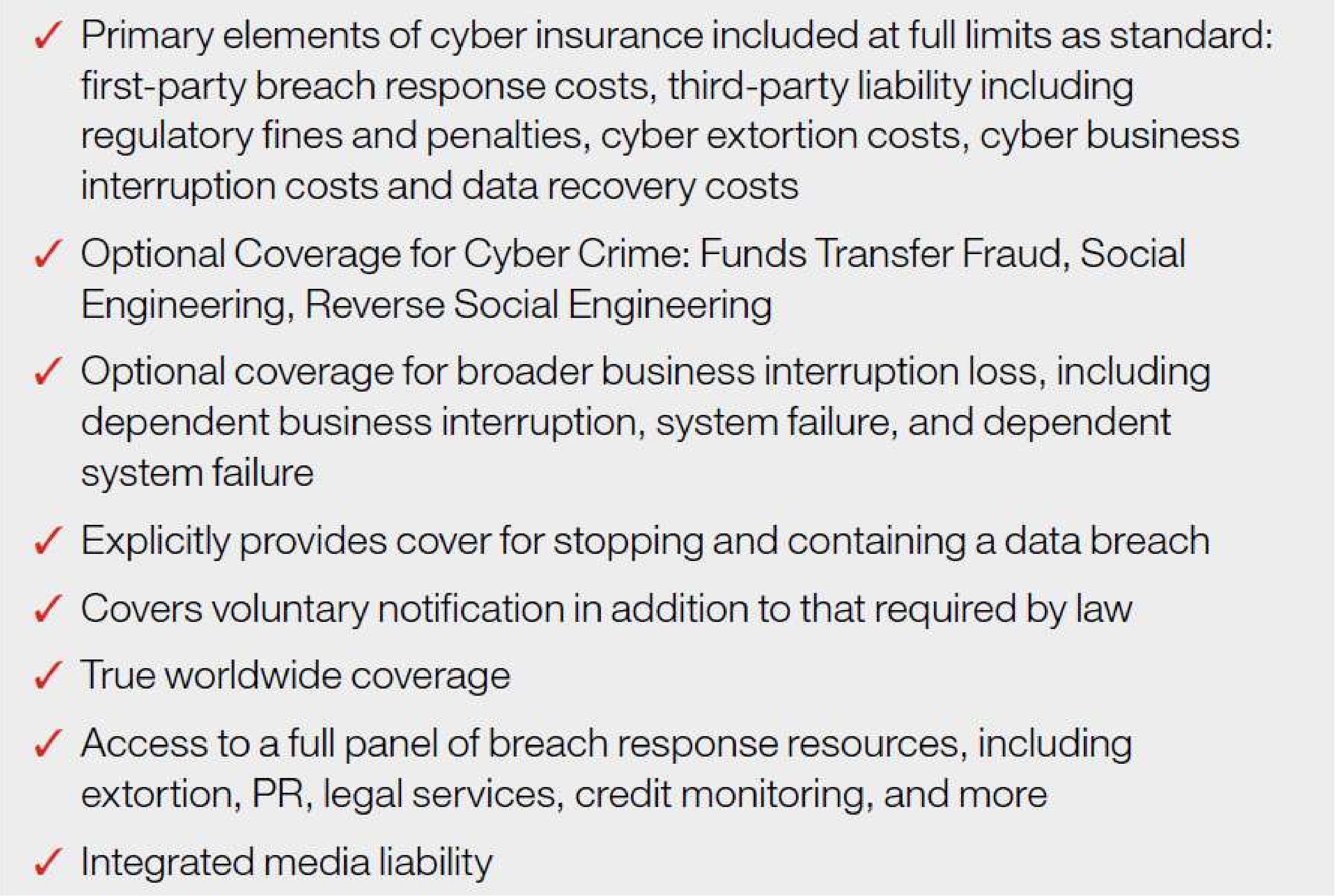
“that causes…reasonably believes has caused, or will cause…

Other Dangers

- **Operational Risk:**
  - **System Failure**
  - **Business Interruption**

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

What is Cyber Insurance



- ✓ Primary elements of cyber insurance included at full limits as standard: first-party breach response costs, third-party liability including regulatory fines and penalties, cyber extortion costs, cyber business interruption costs and data recovery costs
- ✓ Optional Coverage for Cyber Crime: Funds Transfer Fraud, Social Engineering, Reverse Social Engineering
- ✓ Optional coverage for broader business interruption loss, including dependent business interruption, system failure, and dependent system failure
- ✓ Explicitly provides cover for stopping and containing a data breach
- ✓ Covers voluntary notification in addition to that required by law
- ✓ True worldwide coverage
- ✓ Access to a full panel of breach response resources, including extortion, PR, legal services, credit monitoring, and more
- ✓ Integrated media liability

First Party Coverage (that’s you)

- Computer Forensic expenses
- Notification services/expenses
- Credit Monitoring
- Regulatory Fines: HIPAA, Compensatory Awards, PCI
- Public Relations Expenses
- Ransomware & Extortion
- Business Interruption (optional)

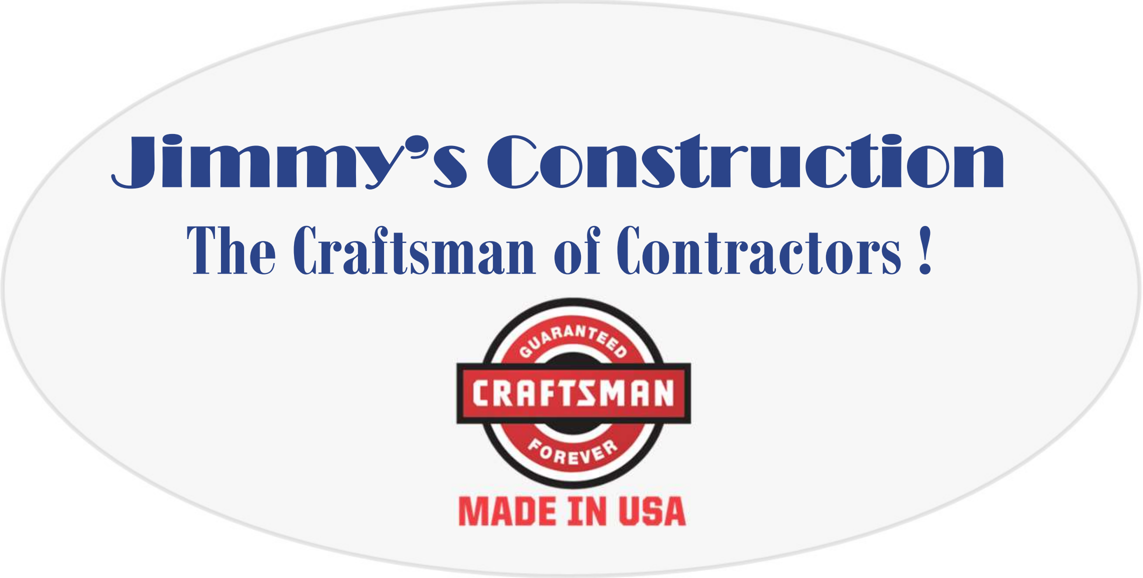
3rd Party Coverage (Clients, Employees, Govt.)

- Payment card reissuance expenses
- Payment card fraud expenses
- PCI Fines/Penalties
- Identity theft lawsuits
- Loss of third party intellectual property or confidential corporate information lawsuits
- Network disruption suits
- Bodily injury arising from lost data
- Mental distress due to exposure of privacy information
- Negligent transmission of a computer virus/worm or malicious code

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations

Media Liability

Coverage available to defend and resolve claims related to online content, such as defamation, trademark or copyright infringement



Jimmy's Construction

The Craftsman of Contractors !

Quote Information

Primary Applicant's name: ____________________

Location address: ____________________

City: ____________________ State: __________ Zip: __________

Web address: ____________________

Email address of primary contact: ____________________

Description of Operations:

Gross revenue for the last fully completed fiscal year: ____________________

Number of records stored containing Personally Identifiable Information:

□ 50,000 or fewer □ 250,000 or fewer □ 500,000 or fewer □ Over 500,000

Data Breach…

It is not a matter of *if*, but *when*.

Questions?

eric@resourcepartnersonline.org

brian@resourcepartnersonline.org

RESOURCE PARTNERS®
RISK MANAGEMENT SOLUTIONS
Serving Peace Church Organizations