Looking Over the Dashboard to the Future: Cyber Liability

Jill Tellez, Professional Liability Leader - Schinnerer
Brad Benjamin, President/CEO – Radium Architecture

Victor O. Schinnerer & Company, Inc.

AIA Continuing Education System

Credits earned on completion of this course will be reported to AIA CES for AIA members. Certificates of Completion for both AIA members and non-AIA members are available upon request.

This course is registered with 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.

Cyber Liability

- Professional service firms are facing an increased exposure to cyber risks and liability through the increased use and dependency on technology.
- While many firms do take the necessary steps to secure their systems, guard their digital assets, protect confidential client information, and maintain productivity,
- Firms that have decided to bypass steps to secure, guard, protect, and maintain their businesses and assets is increasing every day.
- Every firm should have digital protection protocols in place to minimize a data breach and manage in the event a breach occurs.

Learning Objections

At the end of the this course, participants will be able to:

- Understand the evolution of cyber risk assessment and recognize the insurance coverage gap.
- Recognize that a cyber breach could lead to uncovered claims involving the confidentiality of client information, security of those using the facility, regulatory requirements and costs, losses, and damages to the firm.
- Appreciate that not only the architecture firm, but its client and the public are protected against damages to their health, safety and welfare when breach liability and breach rectification coverage is in place.
- Realize the value a data breach team provides to the firm, its clients and the public.

AIA CES Details

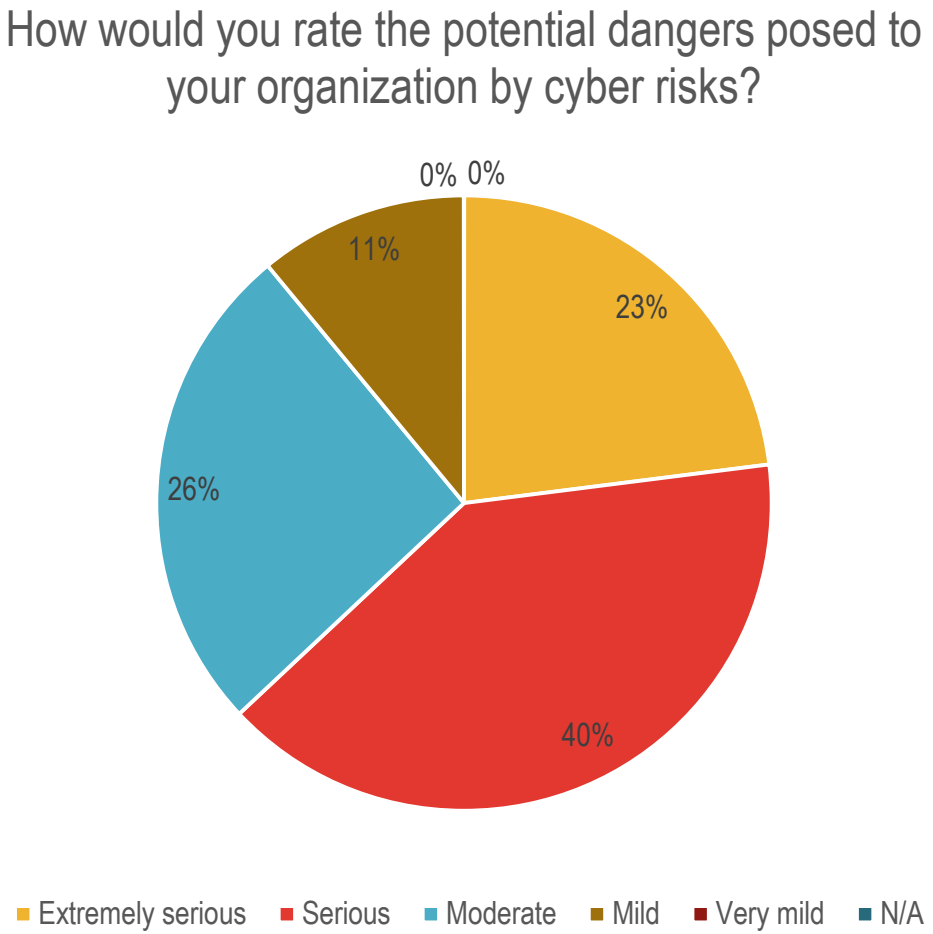
For AIA/CES purposes the provider of this program is:
Victor O. Schinnerer & Company, Inc.
Provider Number: K048

Searching for the Next Pothole: Cyber Liability
Course Number: VOS 604-DE

The speaker for this program is:
Jill Tellez, ARM, Senior Vice President
Victor O. Schinnerer & Company, Inc.
Brad Benjamin, President/CEO
Radium Architecture

November 15, 2016

Perception of Cyber Risk



Source: Advisen, 2015 Network Security & Cyber Risk Management: 4th Annual Survey of Enterprise-wide Cyber Risk Management Practices in Europe

Likelihood & Impact of Risk

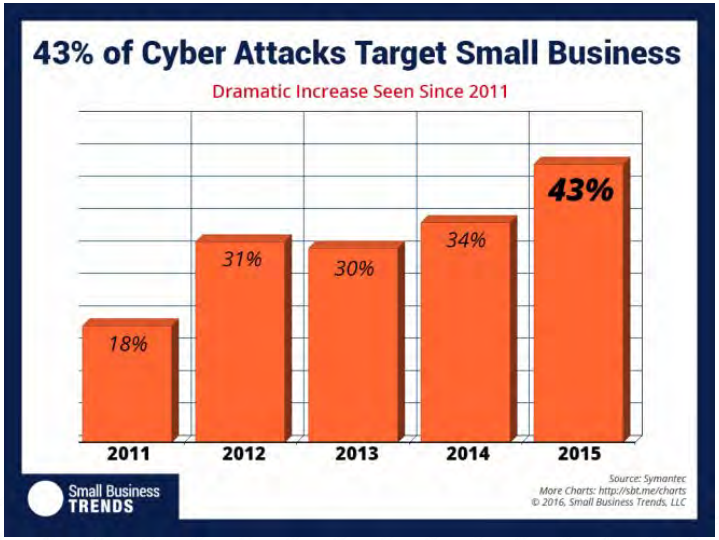
WHO IS VULNERABLE? COMMON MYTHS ABOUT CYBER

Myth #1 Cyber Crime only happens to large companies

Myth #2 My type of business isn't a target

Myth #3 We can self-insure against a network breach

Myth #4 We outsource our network security, data management and payment transactions



The Weak Links

WHAT MAKES SMALL BUSINESSES MORE VULNERABLE?

Cyber Criminals

- Take advantage of People
  - Social Engineering
  - Phishing
- Take advantage of Technology Management Flaws*
  - IT focus is performance, not security
  - Defenses are weak, easily defeated
  - Basic computer hygiene isn't followed
- Take advantage of Management Weakness
  - Security is treated as part of IT
  - Senior management is often not involved and/or clueless on risk or remedies

*Verizon Report – 78% of breaches are low difficulty

Likely Cyber Events

ROOT CAUSES OF RISK

- Malware/ransomware
- Phishing
- Password attacks
- Denial of Service Attacks
- Man in the middle impersonating an endpoint, i.e your bank
- Drive by Downloads
- Malvertising
  Clicking on an infected ad
- Rogue Software masquerading as legitimate/necessary software

Costs of Data Breach

- The average data breach typically results in approx. 29,000 breached records, which cost roughly $201 each. That's $5.85 million for the average single data breach.
- Costs associated with data breaches go well beyond the price of fixing the company security system. From notifying clients to legal settlements, these expenses add up quickly and can include, on average*:
  - Post-breach costs of $1.6 million (Ponemon)
  - Notification costs of $509,000 (Ponemon)
  - Lost business costs of $3.3 million (Ponemon)
  - Legal defense costs of $574,000 (NetDiligence)
  - Legal settlement costs of $258,000 (NetDiligence)
- 60% of small businesses close within 6 months of being victimized by a Cybercrime.

*Risk & Insurance (10/08/2014)

Likelihood & Impact of Cyber Risk

FINANCIAL VULNERABILITY

If a cybercriminal gains access to your network, it will generate loss of productivity, compromise your data and possibly that of your clients, it will impact your company's reputation, and could even result in law suits.

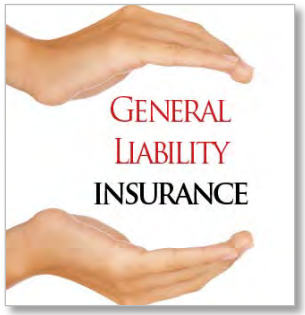
cybernetic-gi.com

Everyone Has Cyber Risk

NOW WHAT?

Evolution of Cyber Risk Insurance Solutions

2000-2016



Early Attempts
Rely on potential coverage from traditional policies.

Recognition of Distinct Risk
Endorsements or wording added to professional policies

Schinnerer's Solution = NetProtect
Covers third party non-professional Cyber Events

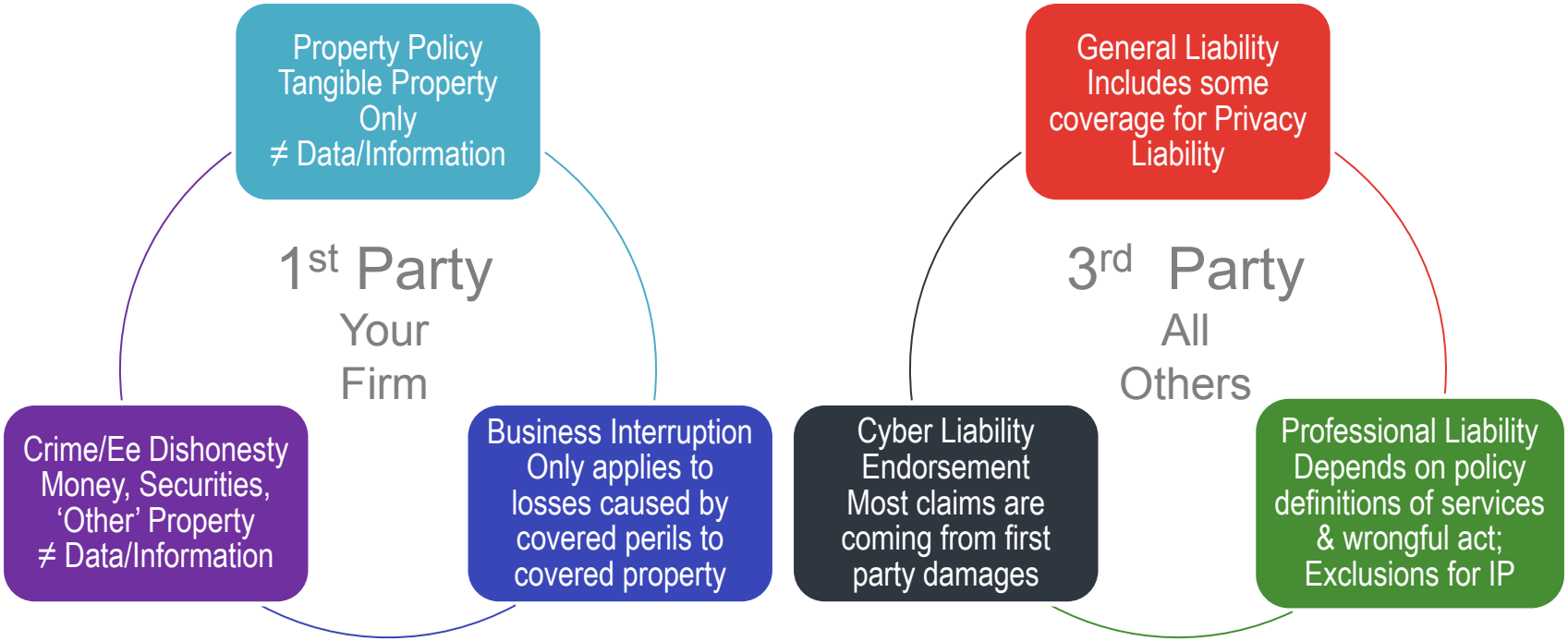
Robust Solution
Stand-Alone Cyber Policy –1st & 3rd Party combined

CONTINUING EDUCATION AIA

VICTOR O. SCHINNERER & COMPANY, INC.

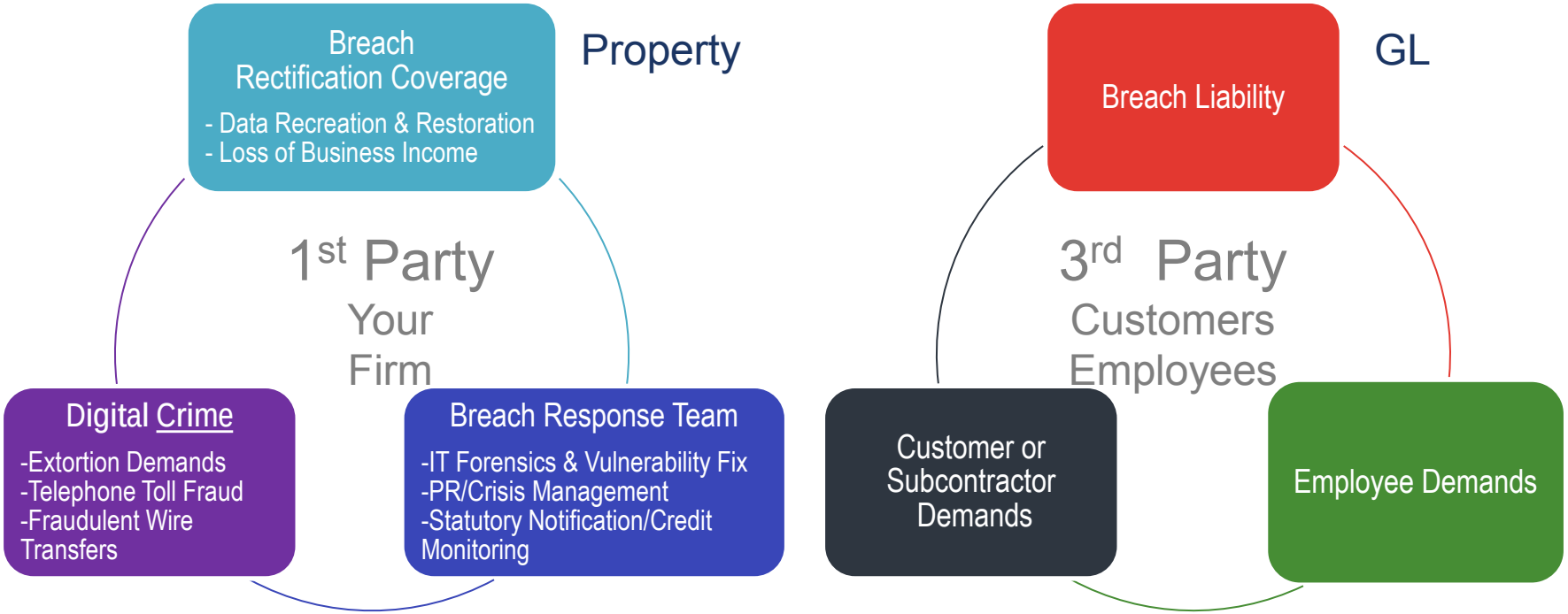
Cyber Risk Transfer

HOW DOES TRADITIONAL INSURANCE RESPOND TO CYBER RISK/EVENTS



Cyber Risk Transfer

WHY A STAND ALONE CYBER INSURANCE POLICY IS THE BEST SOLUTION



CONTINUING EDUCATION AIA

VICTOR O. SCHINNERER & COMPANY, INC.

Cyber Risk Mitigation

NETWORK SYSTEM BEST PRACTICES

- Avoid clicking on links/downloads from untrusted sources
- Verify all requests by email or phone that ask for your password
- Install anti-virus software updates timely, online security/firewall monitoring
- Create strong passwords – change often
- Regularly update and test your system backup
- Use encrypted wireless access points
- Invest in a virtual private network with trusted parties

Cyber Risk Mitigation

INCIDENCE RESPONSE PLAN

THE RIGHT MINDSET – BE READY WITH THE RIGHT TEAM!

- Speed and effectiveness will determine how much damage you may suffer
- IT and others in the organization must know their responsibilities and how to execute on them in crisis mode
- Legal obligations should be identified and planned for in advance
- A communication plan should be planned far in advance

Diary of a Cyber Claim Webinar

Top 10 Mistakes Company Make When Dealing with a Cyberattack

10. Failure to act quickly, learn the facts and address legal obligations.

9. Notify affected parties too soon without knowing basic facts, ensuring system is secure or having resources in place to answer questions.

8. Failure to notify cyber insurance carrier and broker to gather resources and properly manage retention/deductible. Inexperienced vendors for legal, forensics, notification and call center can exacerbate the situation and may not be covered by insurance.

7. Respond without experienced privacy counsel to establish privilege during the investigation and to identify legal duties.

6. Failure to establish an incident response team with decision-making authority who will work closely with the Data Breach Team.

5. Relying on internal IT only. Use third-party experts retained by Data Breach Team.

4. Assume facts and legal interpretations are in your favor without evidence to support such assumptions. This can cloud the investigation and lead to unsupportable messaging.

3. Failure to identify and comply with contract obligations

2. Failure to prepare for litigation and/or regulatory investigation.

1. Failure to assess risks and implement plans to improve security and prevent a future breach.

Looking Over the Dashboard to the Future: Cyber Liability

This concludes The American Institute of Architects Continuing Education Systems Course

---

Victor O. Schinnerer & Company, Inc.

Contact Information:

Andrea Tyler

Andrea.F.Tyler@Schinnerer.com