What, Why, and How of Cybersecurity!

Scott J. Shackelford, JD, PhD, Indiana University
Joe Stanton, Thornburg Agency
Craig Hickman – ProBleu, Inc

I. Cybersecurity 101: What attorneys, financial professionals, insurance professionals, accountants need to know about cybersecurity

Summary and Outline

Cybersecurity literacy is becoming increasingly vital to business executives and leaders across an array of industries, sectors, and nations. Cyber attackers, ranging from hactivists to organized crime networks and even nation states, are targeting vulnerable networks and are frequently successful in stealing funds as well as valuable intellectual property. Congress, international organizations, and industry groups continue to call for cybersecurity best practices to better manage the multifaceted cyber threat facing the private sector. However, it is not always clear what those practices should be, or how to implement them in a dynamic, global regulatory environment.

A. What is "reasonable" cybersecurity, and what role does insurance play in protecting individuals, and firms, from cyber attacks?

B. Now that everything from refrigerators to stock exchanges can be connected to a ubiquitous Internet, how can we better safeguard privacy across networks and borders? This session will explore these issues.

II. Why cyber criminals love professional services and what your industry should do about it

Summary and Outline:

With the enormous amount of sensitive information stored digitally, companies need to take the proper measures to ensure this data is never compromised. Ultimately, it is the responsibility of each business owners to protect their clients' data. Failing to do so can result in a data breach, which costs companies billions of dollars every year. Understanding the risks involved with data security can help you prevent a privacy breach. NetDiligence reports in their 2021 Cyber Claims Study
Report file:///C:/Users/joe/Downloads/NetD_2021_Claims_Study_1.0_PUBLIC.pdf that cybercrime is on the rise in both frequency and severity and professional services such as lawyers, accountants, financial advisors, insurance providers and others in this industry who have high-value data and easy-to access systems are the leading target industry for cyber criminals. In 2021 Professional services had approximately 18% claims (1,088 out of 5,800) that

totaled $229 Million in incident costs with an average cost of $211,000 and claims cost ranging from $1,000 to $120.2 million. Our section will cover why professional services are the leading target and what should be done with the following proposed outline:

A. Typical Challenges and Misnomers
B. What is Data Breach?
C. Four Components of Cyber Risk Management
D. Options for Cyber Liability Insurance Protection
E. Next Steps for Risk Management and Risk Transfer

III. **Cybersecurity - Protecting your Clients and Business**

Summary and Outline:

This section will help attendees learn about what cyber security and attacks are, how they disrupt and destroy business and client relationships and processes, and how to create a structure within your business to protect your process and clients' information.

A. Scared Yet - Rise of Cyber attacks and how it works
   -Why cyber attacks work
   -Results of cyber attacks
B. What to do in order to Protect your Business and Clients
   -What are Cybersecurity Best Practices? What is Risk Management in Cybersecurity?
   -Integrate Network Monitoring and Present Real-Time Solutions
   -Understand Software Design and Secure Practices

Learning Objectives:

1. Objective One: Reviewing the typical challengers and misnomers associated with Data breaches will ensure that the audience is informed on their true cyber-crime exposures not based on what they have or have not experienced so far. This lesson will help each member of the audience identify if their current data breach protocol and encourage them to make adjustments, improvements and/or implement policies and procedures.
2. Objective Two: This lesson will help Audience members identify exposures to Data Breach, be proactive and implement a data breach response plan and to keep informed with ongoing requirements when a data breach has been discovered.
3. Objective Three: Each member of the audience should know how to implement components of Cyber Risk Management into business practice.
4. Objective Four: Each member will develop a basic understanding of the different options for cyber protection and next steps for risk management and risk transfer related to cyber crime.