An aerial photograph of a city, likely Los Angeles, showing a dense residential area in the foreground and a prominent skyline of skyscrapers in the distance under a hazy, blue sky with light clouds.

SecureTheVillage: Turning People and Organizations into Cyber Guardians

Managing Cyber-Risk and Insurance

January 2019

This SecureTheVillage Webinar brought to you by ...

2

PEPPERDINE | GRAZIADIO BUSINESS SCHOOL



Managing Cyber-Risk and Insurance

- Guide: Stan Stahl, PhD
 - ▣ Founder, SecureTheVillage
 - ▣ President, Citadel Information Group
- Guest: Howard Miller
 - ▣ Senior Vice President, Director Technology Division, LBW Insurance & Financial Services
 - ▣ Pepperdine Graziadio CyRP Program Advisory Board
 - ▣ SecureTheVillage Board of Directors

Discussion Topics

4

- Cyber Risk
- The Widening Cyber Exposure Gap
- Risk Mitigation Alternatives
- First Party Cyber Insurance
- Third Party Cyber Insurance
- Insurance Considerations in Hiring an IT Organization

Risk Identification: An Illustration



- Exposure: Human
- Threat: Water Fountain
- Hazards
 - Funneling: Person, Sign
 - Distraction: Cell phone
- Missing Controls
 - Personal Awareness
 - Barrier

How is this like clicking on a link in a phishing attack?

Cyber Risk: The Framework in Which Cyber Insurance Decisions are Made

6

- Typical Buying Questions
 - ▣ Do I buy cyber insurance?
 - ▣ How much?
 - ▣ What coverages?
- Must Be Answered in Context of Risk
 - ▣ Uncertainty of negative effects manifesting that impact ability to achieve objectives
 - ▣ Frequency & Severity
 - How often is it likely to happen
 - How much will it cost

Typical Cyber Risk Coverage Availabilities

7

□ Perils / Causes of Loss

- Network intrusion
- Unauthorized Access
- Unauthorized Use
- DDoS
- Spear-Phishing
- Fraudulent Fax

□ Loss

- Breach disclosures
- BEC and other online fraud
- Theft of intellectual property
- Cyber-destruction of hardware / software
- Ransomware and other cyber-extortion
- Web site copyright infringement

WHAT IS

FIRST-PARTY COVERAGE

AND WHAT SHOULD YOU LOOK FOR?

First-party cyber coverage protects your data, including employee and customer information. This coverage typically includes your business's costs related to:

- Legal counsel to determine your notification and regulatory obligations
- Customer notification and call center services
- Crisis management and public relations
- Forensic services to investigate the breach
- Recovery and replacement of lost or stolen data
- Lost income due to business interruption
- Cyber extortion and fraud
- Fees, fines, and penalties related to the cyber incident

WHAT IS

THIRD-PARTY COVERAGE

AND WHAT SHOULD YOU LOOK FOR?

Third-party cyber coverage generally protects you from liability if a third party brings claims against you. This coverage typically includes:

- Payments to consumers affected by the breach
- Claims and settlement expenses relating to disputes or lawsuits
- Losses related to defamation and copyright or trademark infringement
- Costs for litigation and responding to regulatory inquiries
- Other settlements, damages, and judgments
- Accounting costs

More insurance resources for small businesses available at www.insureuonline.org/smallbusiness

CYBER INSURANCE

Recovering from a cyber attack can be costly.

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs, including whether you should go with first-party coverage, third-party coverage, or both. Here are some general tips to consider.

WHAT SHOULD YOUR CYBER INSURANCE POLICY COVER?



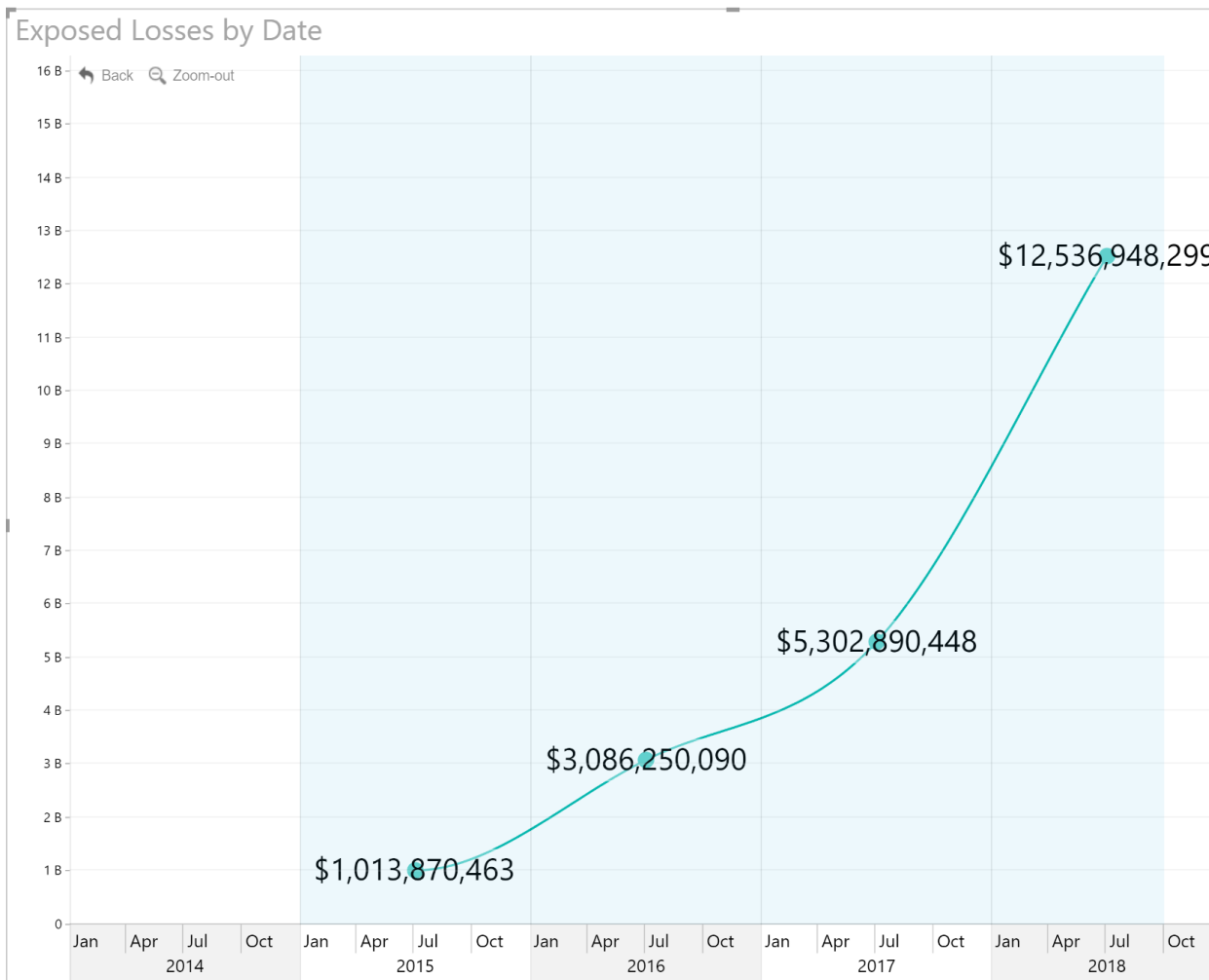
Make sure your policy includes coverage for:

- Data breaches (like incidents involving theft of personal information)
- Cyber attacks on your data held by vendors and other third parties
- Terrorist acts
- Cyber attacks (like breaches of your network)
- Cyber attacks that occur anywhere in the world (not only in the United States)

Also, consider whether your cyber insurance provider will:

- Defend you in a lawsuit or regulatory investigation (look for "duty to defend" wording)
- Provide coverage in excess of any other applicable insurance you have
- Offer a breach hotline that's available every day of the year at all times

Why Cyber-Insurance: Business E-mail Compromise — Four-Year Growth Rate



Source: FBI PSA

Why Cyber Insurance: A Few Data Breach Statistics

11

In 2017, cyber attacks cost small and medium-sized businesses an average of \$2,235,000.

Ponemon 2017 State of Cybersecurity in SMBs

58% of malware attack victims are categorized as small businesses.

Verizon 2018 Data Breach Investigations Report

60% of small businesses say attacks are becoming more severe and more sophisticated.

Ponemon 2017 State of Cybersecurity in SMBs

Taking Control



Looking Both
Ways Means
Paying
Attention

Like noticing
the email isn't
really from
your boss

Risk Management: Framework in Which Cyber Insurance Decisions are Made

13

$$\textit{Residual Risk} = \frac{\textit{Threats*Vulnerabilities}}{\textit{Countermeasures}}$$

Risk management – Five-Step process of managing uncertainty of exposures that affect an organization's assets and financial statements:

1. Identification
2. Analysis
3. Control
4. Financing
5. Administration

Risk Management Framework:

Key Objectives: Prioritize & Protect



$$\text{Residual Risk} = \frac{\text{Threats} * \text{Vulnerabilities}}{\text{Countermeasures}}$$

Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> • Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy • Supply Chain Risk Management 	<ul style="list-style-type: none"> • Identity Management & Access Control • Awareness and Training • Data Security • Information Protection Process and Procedures • Maintenance • Protective Technology 	<ul style="list-style-type: none"> • Anomalies and Events • Security Continuous Monitoring • Detection Processes 	<ul style="list-style-type: none"> • Response Planning • Communications • Analysis • Mitigation • Improvements 	<ul style="list-style-type: none"> • Recovery Planning • Improvements • Communication

Cybersecurity Framework, v 1.1. NIST, 2017

Cyber Insurance “Gotchas”

15

- Definitions, Carve Outs & Exclusions
 - ▣ Information network
 - ▣ Maintenance requirements
- Notification requirements
- Application incorrectly filled out



P.F. CHANG'S[®]

More Risk? Unanticipated Risk. Emerging Risk.

16

THE FTC IS CLOSED DUE TO THE LAPSE IN GOVERNMENT FUNDING.

Learn about the status of FTC online services, website information updates, and the FTC Hearings during the lapse in funding.



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

[Contact](#) | [Stay Connected](#) | [Privacy Policy](#) | [FTC en español](#)



[ABOUT THE FTC](#)

[NEWS & EVENTS](#)

[ENFORCEMENT](#)

[POLICY](#)

[TIPS & ADVICE](#)

[I WOULD LIKE TO...](#)



SOCIAL SECURITY SCAM

TAKE ACTION



[File a Consumer Complaint](#)



[Report Identity Theft](#)



[Get Your Free Credit Report](#)



[Register for Do Not Call](#)



[Get Consumer Alerts](#)

Insurance Considerations in Hiring an IT Organization

17

- Certificate of Insurance
- Required minimum limits
- Workers Compensation
- Professional Liability
- Other Requirements

Information Security Manager & Leadership Team — Getting Started

18

- Identify and Analyze Cyber Risk
- Establish Priorities
- Apply for Insurance
- Work with Consultative Broker
- Integrate with Information Security Management

ResourceKit: Managing Cyber-Risk and Insurance

19

Resources Areas

Cyber Threats

Senior Leadership

Information Security
Management & Governance

The Information Security
Management & Leadership Team

Information Security Policies
and Standards

Information Security Risk
Assessment

Information Classification and
Control

Securing the Human

Managing Cyber-Risk and Insurance

ResourceKit Articles

[Insurance Considerations in Hiring an IT Organization - Certificate of Insurance](#)

Ask the organization to provide a certificate of insurance naming the above entities as Additional Insureds on behalf of the above entities per written contract. A blanket additional insured endorsement is acceptable with language such as: “only where this form is specifically requested by an executed contract” and must be accompanied by [...]

Next Webinar: The Threat Landscape

- Guide: Stan Stahl
 - ▣ Founder, SecureTheVillage
 - ▣ President, Citadel Information Group
- Stan's Guest
 - ▣ Law Enforcement
 - ▣ Private Sector

SecureTheVillage Webinar Series

21

- Information Security Management Guidance
 - ▣ Practical
 - ▣ Real-World
 - ▣ How-To
 - ▣ Actionable
- SecureTheVillage ResourceKit
- First Thursday of month, 10AM Pacific

Information Security Management Webinar Series: Basic Curriculum

22

February 1	Information Security Management Overview; The Role of Leadership
March 1	The Information Security Management & Leadership Team
April 5	Online Bank Fraud — How To Avoid Being a Victim
May 3	Basics of Cyber-Law
June 7	Information Security Policies and Standards
June 29	Conducting an Information Security Risk Assessment
August 2	Information Classification and Control
September 6	Securing the Human
October 4	Managing Security of the IT Infrastructure
November 8	Getting Cyber-Prepared: Incident Response & Business Continuity
December 6	Third-Party Security Management
January 17	Managing Cyber-Risk and Insurance

Webinars: What to Expect in 2019

23

February 2019: The Cybersecurity Threat Landscape

March ... December: Email us with suggestions. What would YOU like?

- The 1st 30-Minutes
- SecureTheHuman
- Securing the Family
- Preparing for the *CA Consumer Privacy Act*

Email: Stan@SecureTheVillage.org

SecureTheVillage: Turning People and Organizations into Cyber Guardians

24

Monthly Webinar Series: Provides Practical Real-World Actionable How-To Information Security Management Guidance.

Executive Focus Groups: Designed to assist Chief Executives understand how to turn their organization into Cyber-Guardians and create a cyber resilient culture.

Information Security Management and Leadership ResourceKit: A practical guide for implementing an information security management and leadership program in your organization.

Code of Basic IT Security Management Practices: A set of basic IT security management practices that are so basic that a failure to implement them puts the organization at a dangerous and unnecessary risk of a costly information incident.

Community-Based Programs to train the broader community in basic cybersecurity defense practices for themselves and their families, helping them become cyber-aware citizens.

Visit us at: SecureTheVillage.org

For More Information ...

25

Stan Stahl, SecureTheVillage & Citadel Information Group

Stan@SecureTheVillage.org

323-428-0441

Howard Miller, SecureTheVillage & LBW Insurance, Tech Secure®

howardm@lbwinsurance.com

(661) 702-6039


FREE *Citadel Cybersecurity News of the Week & Weekend Vulnerability and Patch Report*

<https://Citadel-Information.com>

For Marketing / Sponsorship Opportunities

Email us at info@securethevillage.org. Put *Sponsor Opportunity* in Subject

Visit us at <https://securethevillage.org/sponsorship-opportunities/>



SecureTheVillage: Turning People and Organizations
into Cyber Guardians

Thank You

Managing Cyber-Risk and Insurance

January 2019