

Cyber Risk Insurance for Wholesaler-Distributors

NAW Large Company CFO Roundtable

Steve Robinson | November 7, 2018



Gallagher

Insurance | Risk Management | Consulting



Gallagher

Insurance | Risk Management | Consulting

Agenda

November 7, 2018

- I. Unique Cyber Risk exposures for wholesaler-distributors
- I. The value of Cyber Risk insurance
- II. Beyond insurance – mitigating risk

Unique Cyber Risk Exposures for Wholesaler-Distributors



Gallagher

Insurance | Risk Management | Consulting

It's about more than PII

Unique Exposures

Wholesaler-Distributors – more than PII

- What makes you unique?
 - Data rich environment – business intelligence
 - Reliance upon technology
 - » ERP
 - » Cloud providers
 - » eCommerce
 - » Robotics
 - Extortion threats
 - Margins and the importance of brand
 - Misperception that lower volume PII = lower risk
 - Conduit to retail partners



Unique Exposures

Technology's Ever-Increasing Role

- “We’ve developed a [state-of-the-art platform](#) to make ordering your supplies painless. This innovative and easy-to-use program can be downloaded to your computer, iPhone or accessed online.”
- “Over 99% fill rate on all orders with same day shipment and delivery to 85% of customers within 24 hours. What does that mean? If you order it, you will get it and get it quickly. [Online ordering](#), product information, shop survey requests and Safety Data Sheets are available 24 hours a day, 7 days a week on our website.”
- “With [24/7 access](#) to all of your account information, you can check previous orders and invoices, access a current statement, check branch inventory and [place orders online](#).”
- “[check order status](#), order history, product availability & more.”

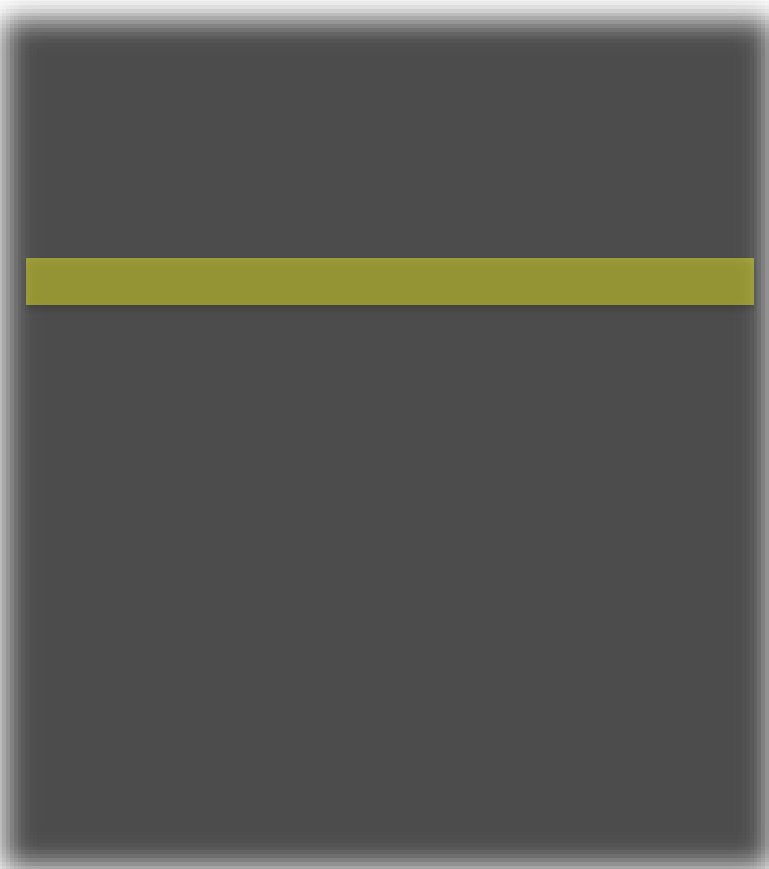


Gallagher

Insurance | Risk Management | Consulting

Threat Vectors

Wholesale Trade – Target for Spam & Phishing

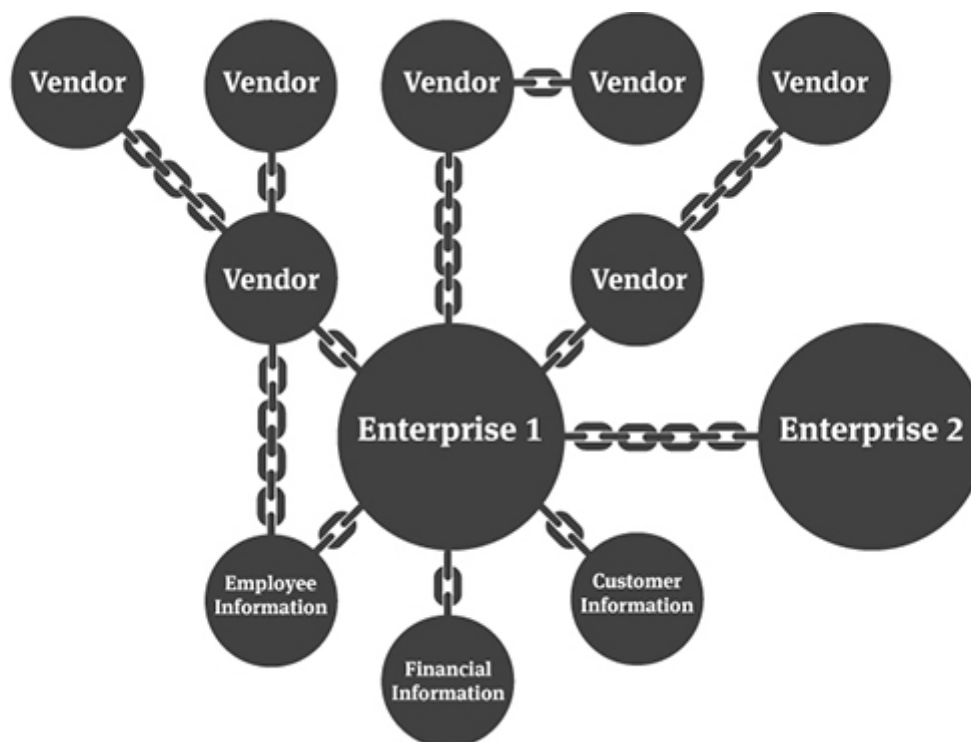


Source: 2018 Symantec Internet Security Threat Report



Wholesale Distribution

Supply Chain

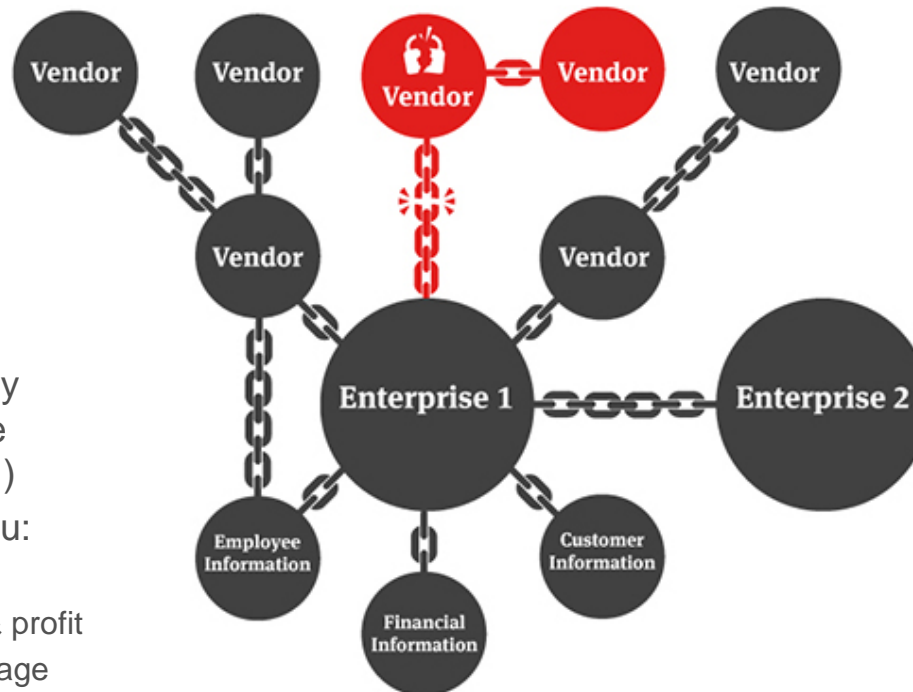




Wholesale Distribution

Cyber Attack on Upstream Supplier

- Key supplier's ops compromised due to cyberattack
- Unable to perform obligations (ie: supply components, provide logistic services, etc.)
- Consequences to you:
 - Delay cost
 - Loss of revenue & profit
 - Reputational damage
 - Downstream customers may terminate agreements, litigate

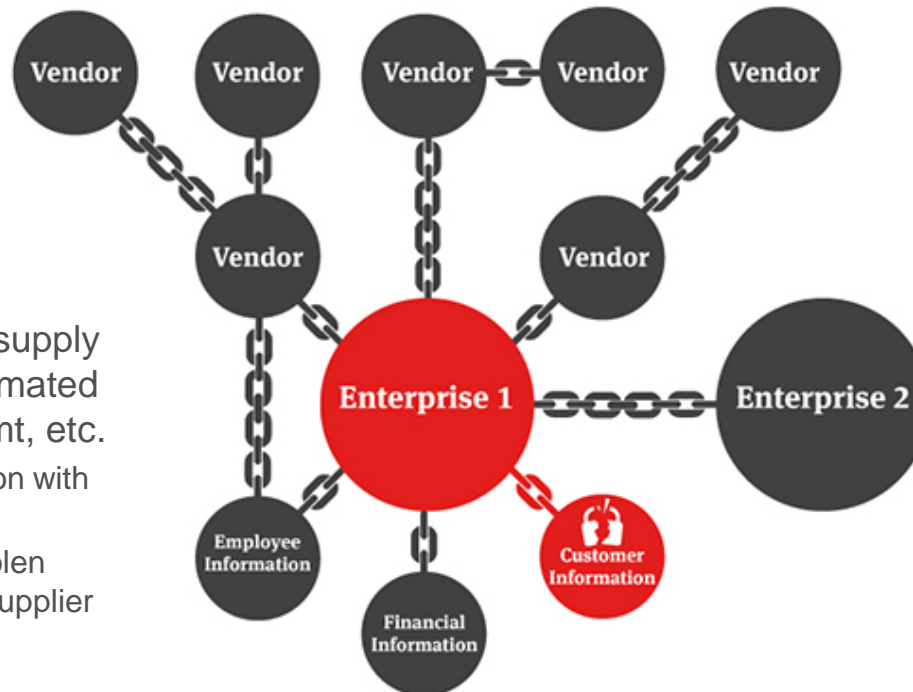




Wholesale Distribution

Data Breaches – System Weaknesses in Supply Chain

- Corporate systems between suppliers & customers
- Close integration of supply chain, enabling automated ordering, invoice pymt, etc.
 - Target – connection with supplier
 - Home Depot – stolen credentials from supplier
- Loss of data via:
 - Sabotage
 - Ransomware



With Innovation Comes Vulnerabilities



Gallagher

Insurance | Risk Management | Consulting

By Shing Hin Yeung - Own work, CC BY-SA 3.0, <https://commons.wikimedia.org/w/index.php?curid=27867977>



Gallagher






Insurance | Risk Management | Consulting

Cyber Risk Insurance

Overview

Overview of Cyber Risk Insurance

30,000 foot view

- Insurance coverage designed to protect a business from:
 - Liability associated with:
 -  Unauthorized release of confidential information
 -  Violation of a person's rights to privacy
 -  Personal injury in an electronic/social media environment
 -  Intellectual property infringement
 -  Violations of state or federal privacy laws
 - Out-of-pocket expenses incurred to make the above problems go away

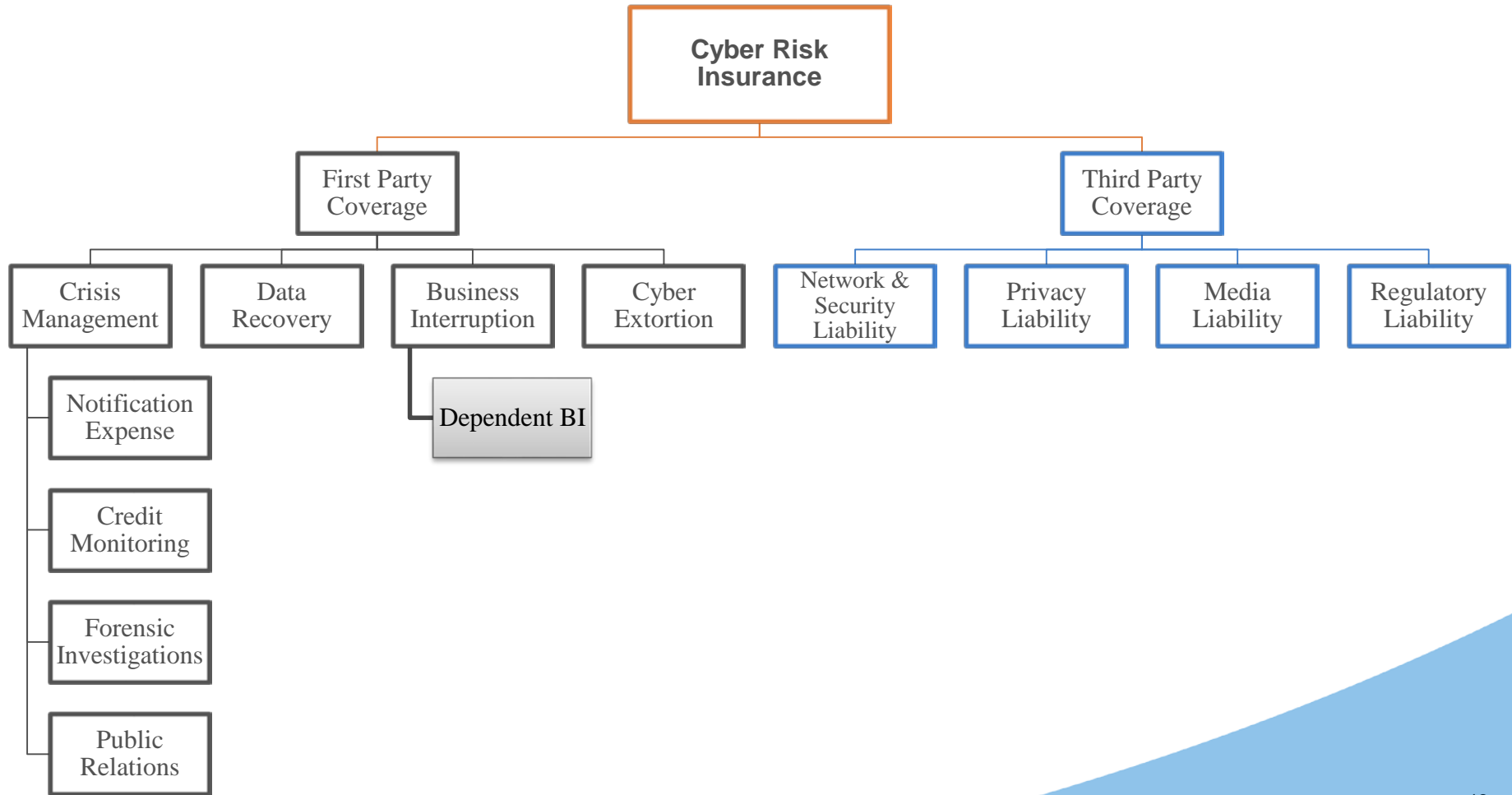
Cyber Coverage Explained

30,000 Foot View



Gallagher

Insurance | Risk Management | Consulting





Gallagher

Insurance | Risk Management | Consulting

Exclusions Create Need

Business Income Exclusions in Property Policies



Evolution of Process & Coverage

Real Data Breaches – Wholesaler-Distributors

Charlotte, NC

The 2017 W-2 forms of employees was fraudulently obtained by a hacker. The information breached included names, Social Security numbers, wage information and mailing addresses. Source: www.privacyrights.org

Lexington, KY

Wholesaler Distributor discovered that it had been the victim of a computer related incident. Unknown individuals targeted corporate website and inserted harmful code. This code allowed unauthorized individuals to monitor the information customers typed into the website when placing an online order. Information of 14,281 customers compromised. Source: databreaches.net

Columbia, SC

Wholesaler distributor victim of email spoofing attack. Email purported to be from CEO. 2017 employee W-2 information. Forensics, legal. Ongoing.

Source: www.idtheftcenter.org

Evolution of Process & Coverage

The Changing Landscape of Cyber Insurance

- Coverage
 - Demand was driven by large, public data breaches of PII – focus on consumer
 - Coverage was designed to meet that demand
 - Data breach vs privacy
 - Social Media
 - Industry built around “breach response” and mitigating consumer impact
 - Notification
 - Call centers
 - Credit/ID monitoring
 - PR
- Process
 - 16-page application
 - Warranties
 - Low adoption rate



Gallagher

Insurance | Risk Management | Consulting

Cyber Risk Insurance

What Has Changed?

Evolution of Process & Coverage

What has changed?

- Threat vectors have expanded beyond commoditization of PII
- Extortion on the rise with increasing reliance on technology
 - The move from random, indiscriminate targets to highly targeted attacks
- Why is this particularly important to Wholesaler- Distributors and how can insurance help?

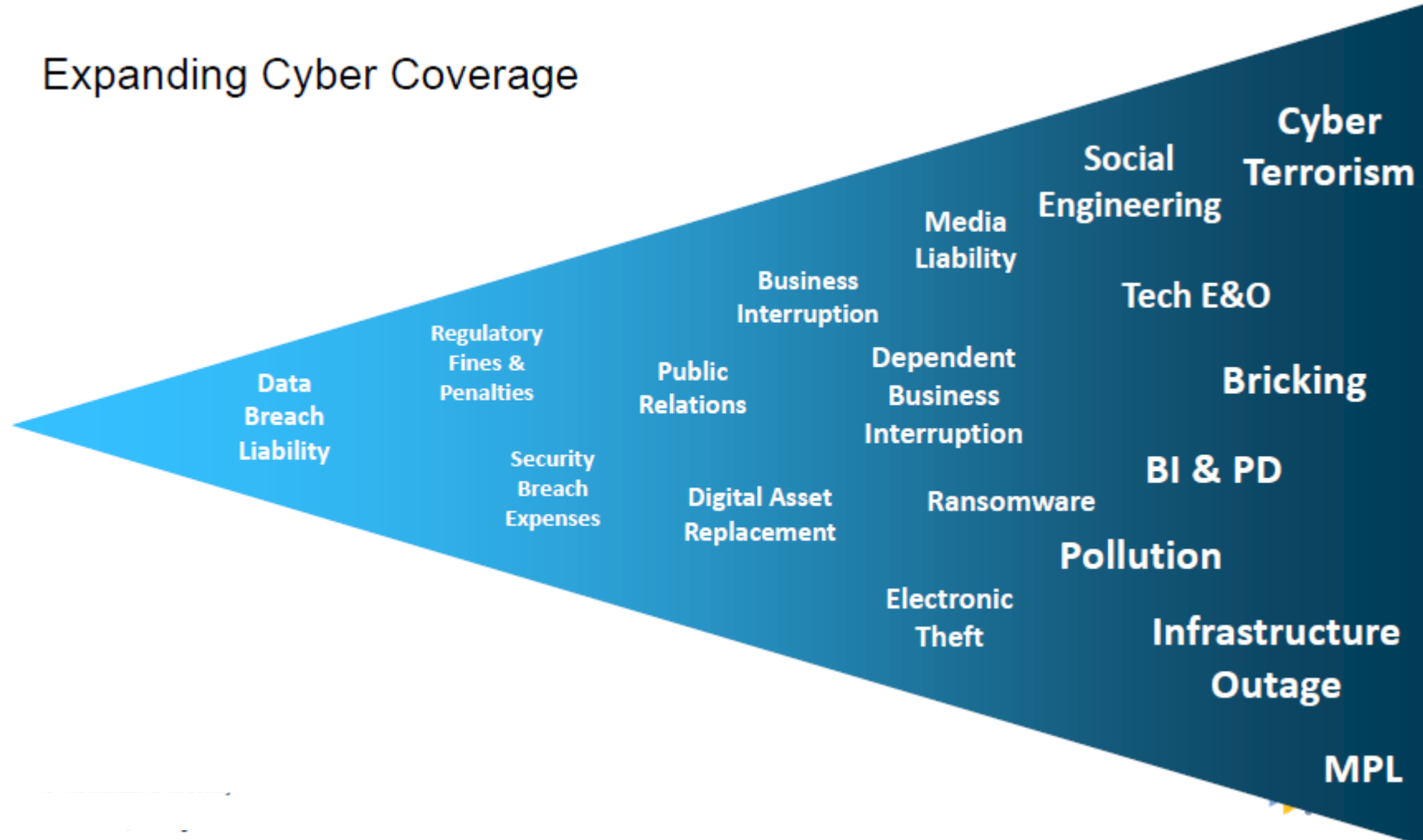


Gallagher

Insurance | Risk Management | Consulting

As Threats Have Changed, Cyber Risk Insurance Has Expanded

Expanding Cyber Coverage



Source: The Institute CPCU Society

© 2017 ARTHUR J. GALLAGHER & CO. | AJG.COM



Gallagher

Insurance | Risk Management | Consulting

The Value of Cyber Risk Insurance

Finances. Operations. Reputation.

- Underwriting process – drastically streamlined
- Shorter apps – warranties
- High capacity = lower pricing
- Enhanced coverage in areas of greatest value to wholesaler-distributors:
 - Business Interruption
 - Reputational Harm
 - Social Engineering
 - Bricking



Gallagher

Insurance | Risk Management | Consulting

The Value of Cyber Risk Insurance

Finances. Operations. Reputation.

- What can the coverage do now that it couldn't do before?
 - Loss of Business Income –disruption of your system
 - ...Or that of your cloud provider
 - System failure/employee error
 - Security breach or system failure of others in the supply chain
 - Reputational harm
 - » Margins and not selling on price alone
 - » A system disruption can affect sales if customers move



The Value of Cyber Risk Insurance

For Wholesaler-Distributors, Reputation is Everything

- “...growth and stability in the market place has been based on a single principle: Great products and attentive service create **lifetime customers**.”
- “Our mission is to continue to be the leader in our industry by providing quality products, superior service and an **unforgettable experience**.”
- “Our biggest return is ensuring that you’re receiving your **highest returns**.”
- “...focused on making the **experiences** of both employees and customers simple, effective and **satisfying**.”
- “We know that our TEAM is our greatest strength, and together we strive to fulfill what we see is our purpose: to **MAKE A DIFFERENCE not only for our customers and each other - but in our industry** and communities as well.”



The Value of Cyber Risk Insurance

Financial. Operational. Reputation.

- What can the coverage do now that it couldn't do before?
 - Social Engineering
 - What is it?
 - Beware:
 - » Conditions
 - » Money/Securities vs Property/Goods
- Bricking
 - What is it?
 - Servers and electronic process control systems

Section D.2. Application of Coverage is amended to include the following:

The coverage provided under Section I.B. Social Engineering Financial Fraud shall apply only if the Insured verifies the instruction to transfer money or securities by following a pre-arranged callback or other established procedural method to authenticate the validity of the request prior to acting upon any transfer instruction.



Gallagher

Insurance | Risk Management | Consulting

Beyond Insurance

Mitigating Risk in Today's Threat
Environment



Gallagher

Insurance | Risk Management | Consulting

Beyond Insurance

Mitigating Risk in the New Threat Environment

- Top Claims Experienced in 2018
 - Ransomware
 - Business Email Compromise (BEC)
 - Social Engineering



Beyond Insurance

Lines of Defense for Ransomware

First Line of Defense: Users

- Security Awareness Training
- Simulated Phishing Attacks

Second Line of Defense: Software

- Firewall
- Antispam/Antiphishing
- Up-to-date antivirus software or advanced endpoint protection
- Software restriction policies on your network to prevent unauthorized applications from running
- Defined patch procedures

Third Line of Defense: Backups

- Backup solution – software/hardware, both
- Ensure all data is backed up regularly
- Segregated from primary networks
- Ensure data is safe, redundant and accessible once backed up
- Regularly test the recovery function of backup/restore procedures



Image Source: Malwarebytes



Gallagher

Insurance | Risk Management | Consulting

Beyond Insurance

Understanding Social Engineering

Organization and user data is at risk everyday because of social engineering attacks



Criminals take advantage of hundreds of years of social conditioning that leads people to trust that others are who they say they are.

Source: www.knowbe4.com



Beyond Insurance

Lines of Defense for Social Engineering



USE STRONG PASSWORDS

- Use at least 3 random words or 1st letter of expression or poem
- Lower and uppercase letters, numbers and symbols
- Minimum of 8 characters
- Use different passwords for different online and system accounts

NEVER USE PUBLICLY AVAILABLE INFO

- Pet's name
- Other family members' name
- Favorite holiday
- Spouse's name
- Child's name
- Place of birth
- Something related to your favorite sports team

Top Ten Passwords most commonly used

1. 123456
2. Password
3. Welcome
4. Ninja
5. Abc123
6. 123456789
7. 1345678
8. Sunshine
9. Princess
10. Qwerty



EDUCATE your team on best practices



Beyond Insurance

Lines of Defense for Business Email Compromise

Attacks against mobile devices and wireless networks continue to rise as employees and consumers use mobile devices and connect to public Wi-Fi

Enable device access security

Enable a passcode, fingerprint or other authentication feature on all mobile devices

Keep OS & apps updated

Recent mobile threats targeted devices with unpatched mobile OS & apps. Apply updates as soon as they are available

Use official app stores

Apps available via untrusted app stores have a higher risk of malware. Only download from official mobile device vendor and corporate app stores

Turn off Wi-Fi & Bluetooth if not in use

Unless needed for a specific purpose, limit access to your location – rogue apps may track you – disable image geo-tagging



Practice mobile & wireless security daily to help protect your information and assets



Global wireless carrier networks are more secure than public Wi-Fi. Connect through your carrier when available.

Connect through a wireless carrier

When public Wi-Fi is only option, verify name of site Wi-Fi network with staff or posted signage before connecting

Verify Wi-Fi name before connecting

When connecting a business device, always use your corporate VPN or other security tools to protect your data

Connect through corporate VPN



Gallagher

Insurance | Risk Management | Consulting

Beyond Insurance

5 Types of Business Email Compromise

1. High level executive fraud
2. Vendor invoice fraud
3. Attorney fraud
4. Employee account fraud
5. Information request fraud



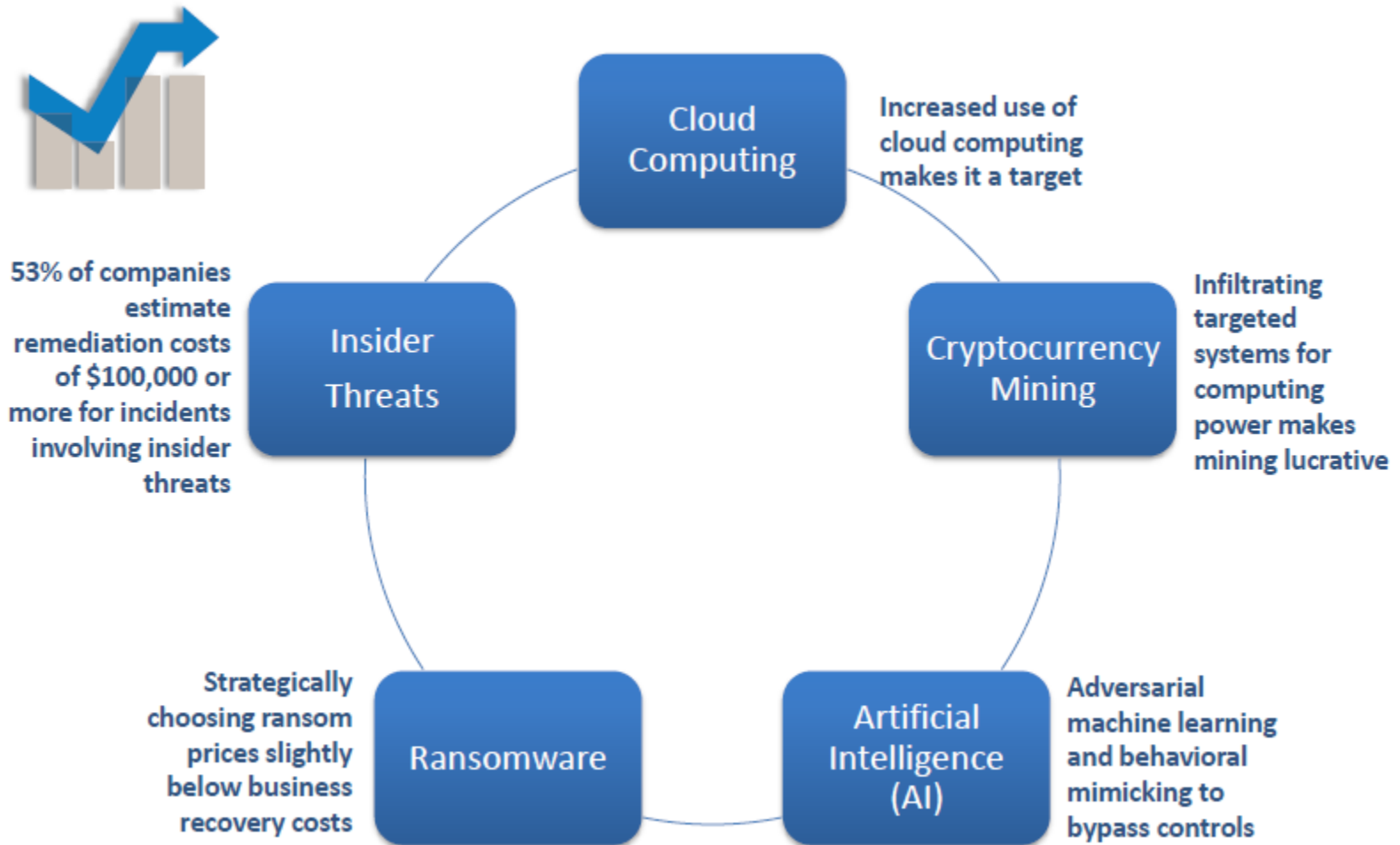
Beyond Insurance

Lines of Defense for Business Email Compromise

- Consistently educate employees
- Always require multi-level authentication for sensitive accounts
- Confirm all requests for money by phone or in-person
- Don't use a free email server
- Run regular "spoof tests"
- Always double-check emails sent from executives
- Verify changes in vendor payment location
- Pay attention to your customers' habits and preferred payment methods
- Delete all spam and never click on links from email addresses you don't recognize
- Work with a managed IT security company if internal resources are inadequate



2018 Trends





Gallagher

Insurance | Risk Management | Consulting

Predictive Modeling

Sample





Gallagher

Insurance | Risk Management | Consulting

Predictive Modeling

Sample





Summary

Cyber Risk Insurance

- As Cyber Risk insurance has evolved to meet the real needs of wholesaler-distributors, demand is increasing
- Risk management and Cyber exposure predictive modeling is evolving as well
- Coverage is more affordable than ever
- Wholesaler-Distributors need to re-think exposure to Cyber Risk in light of today's threats
- Work with a broker who is well versed in Cyber Risk insurance to ensure your coverage meets your needs



Gallagher

Insurance | Risk Management | Consulting

Thank you.

Steve Robinson
National Cyber Practice Leader
Risk Placement Services, a division of Gallagher
Steven_Robinson@rpsins.com
(410) 901-0704

Risk Placement Services is a division of Gallagher. The information and descriptions contained in this presentation are intended as general information and are not complete descriptions of all terms, exclusions and conditions applicable to the products and services offered by Risk Placement Services or any insurance company represented by us. This is not a guarantee of coverage. The information contained throughout this summary is not an insurance policy or contract of insurance. The insurance coverage afforded by RPS is subject to the terms and conditions of the policies as issued. Any reference to pricing is for illustrative purposes only. Actual pricing is subject to underwriting review and acceptability, and, may vary from pricing ranges represented herein. This discussion is not legal advice. RPS does not provide legal advice and highly recommends that insureds seek legal advice of qualified legal counsel in order to become fully apprised of the legal implications related to these issues.

