The Evolving Cyber Market

ICMIF Americas Conference 2017

CYBERSCOUT®

1

Who is CyberScout?

Educate. Protect. Resolve.

For over 14 years, CyberScout has set the gold standard for identity and data defense services. Our longstanding reputation, industry expertise and scalable approach offer businesses and their customers a trusted ally for:

- Identity Management
- Breach Education, Preparation, Response & Remediation
- Fraud, Credit and Reputation Monitoring
- Cyber Security and Data Privacy Consulting

CYBERSCOUT

3

Current Global Reach

660+
Institutions

17.5
Million Households

45
Million Individuals

770,000
Breach Services Customers

CYBERSCOUT

2

Understanding the Risks

Data Breaches in the Headlines

Three Mobile cyber hack: six million customers' private information at risk after employee login used to access database

500 million Yahoo accounts breached

Security

Sports Direct hacked last year, and still hasn't told its staff of data breach

UK firms could face £122bn in data breach fines in 2018

Hackers publish contact info of 20,000 FBI employees

Energy facility cyber incidents rose nearly a third last year, DHS says

UCF data breach: 63K Social Security numbers compromised

Monday 13 March 2017 1:36pm

Three Mobile cyber attack: Mounting numbers of customers hit following November breach

Cyber-Safe

Cyber thieves siphon tax forms from ADP payroll data

NEWS

Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords

The Switch

The human problem at the heart of Snapchat's employee data breach

CYBERSCOUT

How Data Exposures Happen

Employee Error

"University Employee Inadvertently Publishes Personal Information of Students Including SSN Online"
- SC Magazine

Document Disposal

"Samaritan Health Services Investigates After Medical Records Found in Trash"
- Gazette-Times

Hard Drive Disposal

"Company Fined for Leaving Electronic Health Data on Hard Drive of Leased Photocopier"
- CNS News.com

Unauthorized Access

"Florida Health Employee Caught Photographing Patient Data, Gets Fired"
- SC Magazine

CYBERSCOUT

How Data Exposures Happen

Hacking

"1.4 million Users' Information Stolen, Including Payment Card Data"
- IB Times, UK Edition

Loss or Theft

"Laptops With Patient Data Stolen From Medical Clinic"
- WSPA.com

Mailing Error

"Medical Center Mails 63,000 Letters Containing Personal Information to the Wrong People"
- SC Magazine

Third-Party Vendors

"Hospital's Wellness Program Vendor Experiences Data Breach Exposing Employee Personal Information"
- SC Magazine

CYBERSCOUT

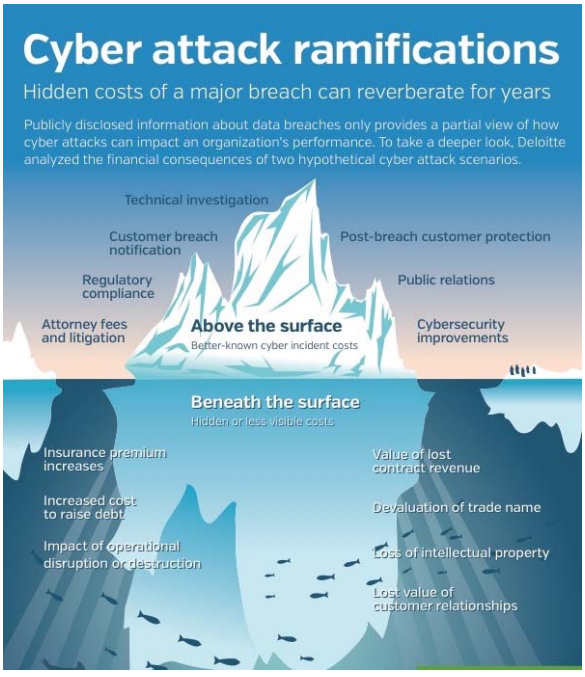
Common Cyber Attacks & Exploits

- Social Engineering
- Ransomware
- DDoS/DoS Attacks
- Zero Day Vulnerability
- Malware/Malicious Code
- Spyware
  - Key logger
- Spoofing
- The “Ishes”
  - Phishing, Spear-phishing, Vishing, SMiShing and Whaling

CYBERSCOUT

In 82% of cases, attackers compromised an organization within minutes

- “Data Breach Investigations Report,” Verizon



A 2016 study from Deloitte dissects well-known and not so well known costs of a cyber attack. The below-the-surface costs can be long-running and devastating.

Examples include:

- Lost customer relationships
- Reputational impact
- Customer protection
- Notifications
- Business Interruption

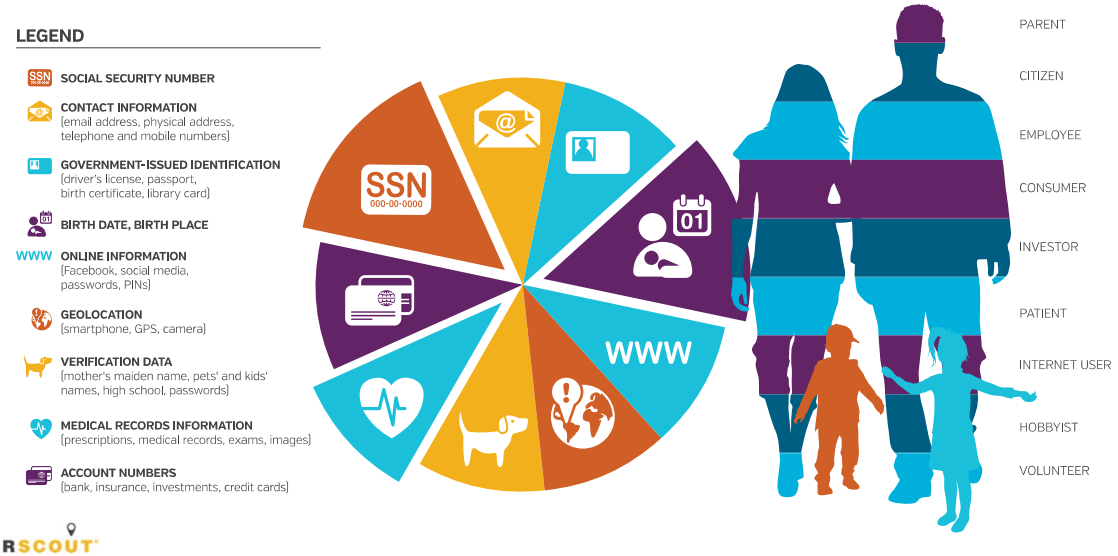
Who are Cyber Criminals Targeting?

- **Large companies** collecting, storing or transmitting sensitive data
  - Insurance carriers, financial institutions, employee benefit providers, governments, hospitals, etc.
- **Small and mid-sized business (SMB)** from brick and mortar locations to online services.
  - 28 million small business owners have no confidence in their security[1]
  - 43% of cyber-attacks worldwide struck companies with less than 250 workers[2]
  - 1 in 5 SMBs reported a cyber-attack[3]
  - 48% reported cyber attacks caused service interruption[4]
  - Average cost of a breach for small to mid-size businesses was just over $180K[4]
- **End Consumers (Individuals)**
  - From human error –a lost wallet -- to emerging risks like the Internet of Things, mobile devices, connected homes and DDoS attacks

The short answer is EVERYONE is a target!

CYBERSCOUT

What Information is at Risk?



CYBERSCOUT

Businesses Handling PII Are At Risk

Employee Records

- Contact Information
- Govt-issued ID
- Birth Date, Birth Place
- Account Numbers

Payment Info

- Online Information
- Contact Information
- Account Numbers

Loyalty Cards

- Online Information
- Contact Information
- Birth Date, Birth Place
- Account Numbers
- Verification Data

3rd Party Vendors

- Contact Information
- Govt-issued ID
- Birth Date, Birth Place
- Account Numbers
- Online Information
- Verification Data
- Medical Records Info

CYBERSCOUT

Sample Industries At Risk

Construction

- Employment data
- Drug tests
- Medical records Payment info
- Intellectual Property

Real Estate

- Employment data
- Social Security Numbers
- Gov't-issued IDs
- Credit reports

Trucking

- Employment data
- GPS-tracking
- Payment info

CYBERSCOUT

Defining the Problem

- **Breaches can be terrifying** for individuals and businesses alike.
  - *Victims need access to valuable preventative education, proactive protection services, and swift and appropriate incident remediation solutions.*
- **Victims need a trusted partner** who goes above and beyond to achieve a successful resolution.
  - *Insurance carriers, financial institutions and employers are often the first place victims look for assistance/guidance.*
- **Lost business is the biggest financial consequence** to organizations that experience a data breach.
  - *Following a data breach, organizations need a partner to help them take steps to retain customers' trust to reduce the long-term financial impact.*

CYBERSCOUT

Defining the Problem

- **Cyber security regulations are evolving** and organizations need expert guidance about staying compliant and competitive.
  - *As regulators shift their focus from post-breach guidance to pre-breach requirements to mitigate risk, organizations of all sizes need experts to help them prepare for changes.*
- Organizations that make improvements to their **data governance programs can reduce the cost of a data breach**.
  - *Development of incident response plans, appointment of a CISO, employee training and awareness programs, and a business continuity strategy – all result in cost savings.*

CYBERSCOUT

3

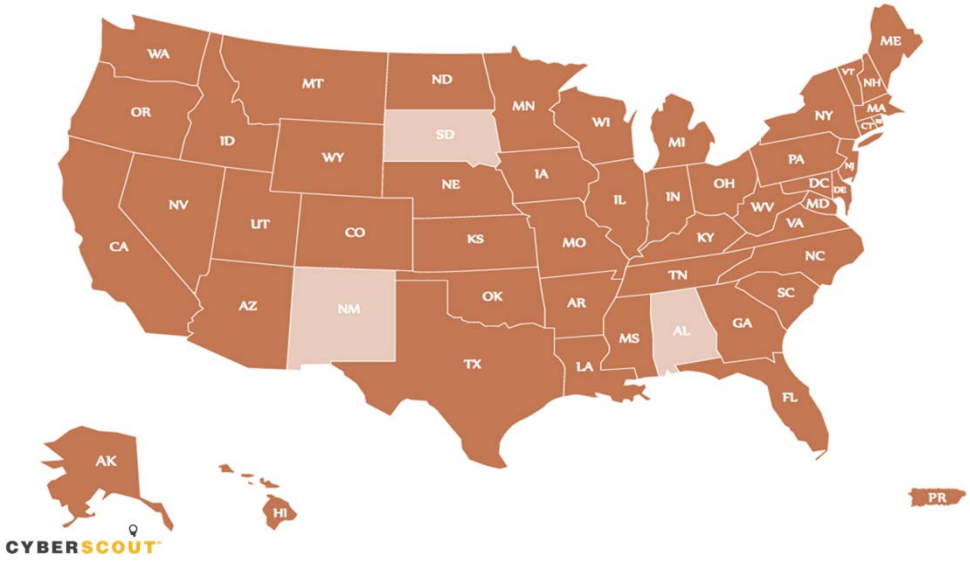
The Evolution of Privacy & Data Breach Regulations

OECD Originated Regulatory Approach

8 core principles for data controllers to abide by under regulation:

CYBERSCOUT

U.S. Cyber begins with Breach Notification Laws



48 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands require notification of security breaches involving PII

CYBERSCOUT

The Next Wave of Cyber Regulations

- **Canada**'s Digital Privacy Act modifying the Personal Information Protection and Electronic Documents Act (PIPEDA) adding data breach notification and reporting requirements
- The **New York** Department of Financial Services (NYDFS) rules that require DFS-regulated entities to adhere to stringent cyber security requirements
- The **European Union** General Data Protection Regulation (GDPR) that strengthens data protection for individuals in the E.U. adding data breach notification and reporting requirements
- The E.U.-U.S. Privacy Shield replacing Safe Harbor program to provide more rigorous protection of personal data to facilitate digital commerce across the Atlantic
- **Japan**'s Amended Act on the Protection of Personal Information (December 2016, goes into full effect on May 30, 2017)
- **Argentina**'s DPA releases proposed Bill to update existing regulations making DPA an independent regulator with more power

CYBERSCOUT

Current Latin American Data Breach Regimes

CYBERSCOUT®

1

Latin American Data Breach Requirements

Latin American Breach Notification

Countries with breach notification (Mandatory Notice)

Key:	✓	⚠	✗
Texts in force	Texts in force	Bill Pending	No requirement

Country	Mandatory notification required	Notification: to consumer	Notification: to regulatory authorities	Notification: to other agencies
Latin America				
Chile	✓	✓	✓	✗
Colombia	✓	⚠	✓	✗
Costa Rica	✓	✓	✓	✗
Ecuador	✓	✓	✓	✓
Mexico	✓	✓	✗	✗
Uruguay	✓	✓	✗	✗

CYBERSCOUT

23

2

Latin American Data Breach by Country

Chile

- **First Latin American country to enact a data protection law**
- Law No. 19,628 sobre *Proteccion de la Vida Privada* (1999)
  - Absence of ***any*** provisions relating to data breach notification requirements
- Data breach notification requirement loosely applied from the Chilean Consumer Act
- Law No. 19,496 (1997)
  - Article 46 requires that a service provider notify its customers in cases of contingencies or risks associated with its product or service.
  - Article 3 grants consumer rights to service/product safety and provides for redress via compensation for damages
  - NO specific provision requiring personal data breach notification
    - The obligation is inferred; no specific conditions for notification

CYBERSCOUT

25

Costa Rica

- **Law on Individual Protection for Processing of Personal Data ('the Law') and Executive Decree N° 37554**
- Article 38 of the Decree regulates general data breaches
  - *"Any irregularity in the treatment or storage of the data, such as loss, destruction or any similar data breach."*
- Article 39 indicates that the data controller (i.e., the party responsible for the data) must inform the data subject and the Data Protection Authority of any security vulnerabilities that have arisen
  - Within five (5) business days
    - ✓ Required notice to data subjects and DPA
    - ✓ Comprehensive review must be initiated to determine extent of problem and any corrective and preventive actions

CYBERSCOUT

26

Ecuador

- **NO clear breach requirement; covered instead under *several* different overlapping regulations including:**

➢ The Constitution of the Republic of Ecuador
  - Guarantees protection of personal data including access and restrictions on the collecting, storage, processing, distribution and circulation.

➢ Organic Law of the National System of Public Data Register
  - Defines personal data as: ideology, political affiliation, ethnicity, health status, sexual orientation, religion, credit and financial information, and any other data related to the privacy and intimacy of the person.

➢ Organic Law of Civil Data and Identity Management
  - Creates a personal data registry ('Registro Personal Único' [RPU])

➢ Electronic Commerce, Data Messages and Electronic Signatures Law

CYBERSCOUT

27

Mexico

- The *Federal Law* and *Regulations on the Protection of Personal Data Held by Private Parties* requires breach notification to data subjects under specific circumstances

➢ Security breaches occurring at *any stage of the processing*, which significantly affect the property or moral rights of a data subject shall be informed immediately by the controller to the data subject, so that he/she can take appropriate action to protect his/her rights.

  - Security breaches which may occur in *any stage of the processing* are:
    - ✓ loss or unauthorized destruction;
    - ✓ theft, misplacement or unauthorized copying;
    - ✓ unauthorized use, access or processing; or
    - ✓ unauthorized damage, alteration or modification.

CYBERSCOUT

28

Mexico

- The Regulations state that the data controller must notify the data subject of at least the following:
  - ✓ Nature of the breach;
  - ✓ Personal data compromised;
  - ✓ Recommendations to the data subjects concerning measures they can adopt to protect themselves;
  - ✓ Corrective actions implemented; and
  - ✓ How data subjects can get more information regarding the breach.
- Currently:

➢ DPA notice not required, only notice to data subject(s).

➢ DPA has not issued any clarification regarding what should be considered a *"significant" damage to property or moral rights of the data subjects*.

CYBERSCOUT

29

Uruguay

- Breach notification is rather loosely applied with the exception of specific requirements for telecoms.
- Similar to the breach notice requirements for telecoms in the E.U.
- *Law 18.331 on Personal Data Protection and Habeas Data Action* and *Decree 414/009* regulates requirements for protection of personal data

➢ Article 10 specifically regulates security measures to protect personal data and ensure its integrity, confidentiality and availability. The Decree also states the notification requirement for general data breaches.

➢ Article 20 refers to the protection of personal data *specifically* in the telecoms sector.

CYBERSCOUT

30

4

What is Cyber Coverage?

Cyber Insurance Trends

- Cyber insurance is a potentially huge, but still largely untapped opportunity for insurers and reinsurers
- Any organization that stores and maintains customer information (PII), collects online payment information, or uses the cloud should consider cyber insurance
- PwC estimates that annual gross written premiums are set to grow from around $2.5 billion today to $5 billion in 2018 and could reach $7.5 billion or higher by 2020
- 90% of cyber insurance is purchased by U.S. companies but only around a third of companies in the U.S. have some form of cyber coverage
  - There is a wide variation in take-up by industry, with only 5% of manufacturing companies in the U.S. holding standalone cyber insurance, compared to around 50% in the healthcare, technology and retail sectors
- In the UK, only around 2% of companies have standalone cyber insurance

CYBERSCOUT

Source: PwC Insurance 2020 & beyond: Reaping the dividends of cyber resilience

Cyber Insurance Markets

THE NUMBERS

32+	30+	9+
Domestic Markets	Lloyd's syndicates	Bermuda Markets

16	Number of years that a dedicated policy has been offered
$3B	Total estimate of current annual premium placed in the market
$500M	Largest cyber stand-alone program placed in the market
27%	Increase in purchasers in 2016, following 32% and 21% in years prior

CYBERSCOUT

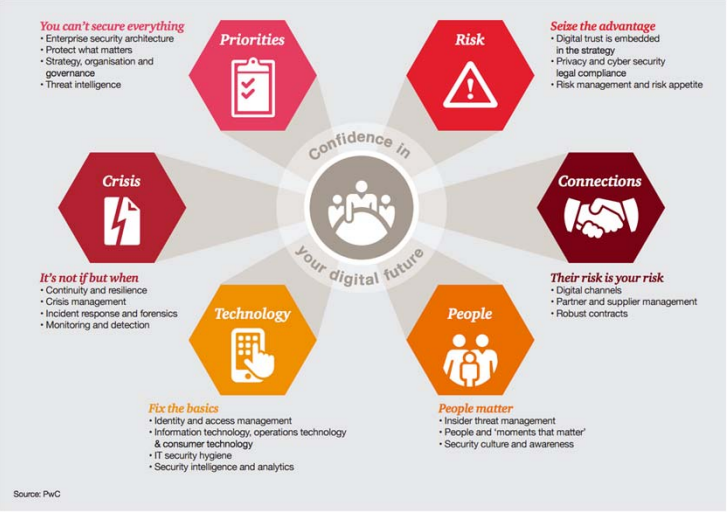
Cyber Insurance Overview

- A cyber (risk/liability) insurance policy is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event.
- Origins in errors and omissions (E&O) insurance by tech companies was expanded to address
  - software product bringing down another company's network
  - unauthorized access to a client system
  - destruction of data
  - virus impacting a customer.
- Cyber insurance today covers expenses related to first parties as well as claims by third parties
  - Addresses forensic investigations, business losses, data breach notification costs, and legal representation.
- Insurers use different terminologies -- making the policies difficult to read and compare.

CYBERSCOUT

Cyber Insurance Trends

- Cyber insurance **capacity will continue to increase**
- **Creates downward pressure on premium rates**
- Some insurers may compete by relaxing limits, exclusions and other terms and conditions
- Important to understand the **motivations and drivers** behind why businesses are purchasing cyber coverage along with their **potential risks**



CYBERSCOUT

Insuring Agreements Explained

Third Party Coverage	**Errors & Omissions (E&O)**	Coverage for defense costs and damages arising out of allegations of acts, errors, omissions or negligence in providing services to others. Can include specialized Tech E&O or Miscellaneous Professional Liability cover.
	Security/Privacy	Coverage for defense costs and damages arising out of a 1) failure or violation of the security of a computer system or network or 2) a failure to protect confidential information or any violation of a federal, state, foreign or local privacy statute. Can include coverage for PCI fines, penalties and/or assessments as well.
	Regulatory	Coverage for costs to respond to a governmental investigation arising out of a privacy event. Includes coverage for fines and penalties to the extent allowed by law.
	Media	Coverage for third party claims alleging libel, slander, copyright/trademark infringement, invasion of privacy, etc. arising out of all content distributed by a company.
First Party Coverage	**Breach Response**	Coverage for costs to respond to a data breach, including costs to conduct an investigation (including forensics costs) as to the cause of the event, public relations costs, notification costs, costs to offer credit monitoring/ID Theft services.
	Network Interruption	Coverage for loss incurred by the insured following a security failure (usually after a waiting period and subject to a monetary retention). Insurable costs can include extra expense caused by the interruption and lost revenue.
	Data Restoration	Costs to restore/recreate electronic data after a failure or violation of the security of a computer system.
	Cyber Extortion	Coverage for loss incurred by the insured for money paid with the insurer's consent to resolve a cyber security threat and costs to investigate the cause of the threat.

36

Ancillary Coverages Explained

Coverage

Employed Lawyers (CCP)	Liability coverage for defense costs and damages arising out of the work done by employed corporate lawyers. Includes coverage for lawyers' actions while providing moonlighting and pro bono services.
Reputation Guard	First party coverage for public relations costs incurred responding to any act or event that, if or when disclosed in a publication and seen by the company's stakeholders, could have an adverse impact on public perception of the insured.
System Failure	Broadens the first party trigger for network interruption coverage from security failures (e.g. hacks) to any unintentional outage (e.g. computer glitches).

CYBERSCOUT

37

Coverage Types

Privacy Breach Expense

- Legal
- Forensics
- Crisis management
- Notification
- Call center support
- Credit monitoring
- Fraud remediation
- PR assistance

First-Party Cyber

- Providing assistance for data restoration or re-creation, digital assets
- Business interruption
- System/admin failure
- Fund transfer fraud
- Cyber extortion
- Virus removal

Liability

- Defense and settlement costs
- Fines
- Penalties
- Network security
- Media liability
- Defamation

CYBERSCOUT

Cyber Insurance Supporting Services & Tools

- Proactive Fraud & Credit Monitoring
- Breach Education, Response & Remediation
- Identity Management & Resolution Services
- Cyber Security & Data Privacy Consulting

CYBERSCOUT

Cyber Liability Program Solution for Commercial and Personal Lines

- Underwriting / Risk Evaluation
- Program Development
- Regulator / Filings
  - Underwriter Training
  - Agent Training
  - Claims Training
- Coverage
  - Experience / Product Pricing
- Marketing Support
  - Implementation
- Claims Consultation / Mitigation
  - Loss Control Support / Resources

CYBERSCOUT

Portfolio Analysis

Exposure	Analysis of your specific risk portfolio
Hazard Grade Assignment	Your book of business categorized by Cyber risk
Pricing	Weighted composite premium: low, medium, high hazard grades

CYBERSCOUT

Hazard Grades

Low
- Insured has a website for informational purposes only

Medium
- Insured conducts business, at least partially, over their website and/or store credit card numbers as well as other fairly sensitive information

High
- Insured will either conduct all of their business through their website or store highly sensitive information or some combination of both

Excluded
- Insureds that are ineligible for an opt-in program

CYBERSCOUT

The Next Wave of Cyber Coverage: Personal Cyber Coverage

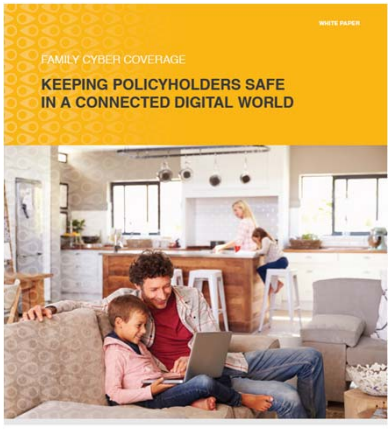
- Connected technology is reshaping the threat landscape in households.
- Even for technically savvy people, keeping up with protections against cyber threats can be a constant challenge.
- Cyber crime losses in the U.S. alone are nearly double that of property crimes – $30 billion vs. $14 billion.
- Cyber protection can help families offset financial and emotional costs of cyber crime.

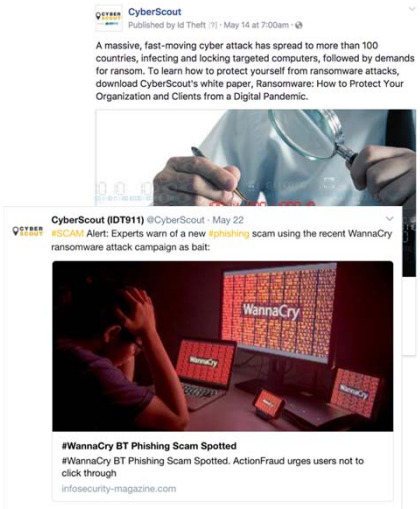
Insurers have the opportunity to educate and provide tools to address:

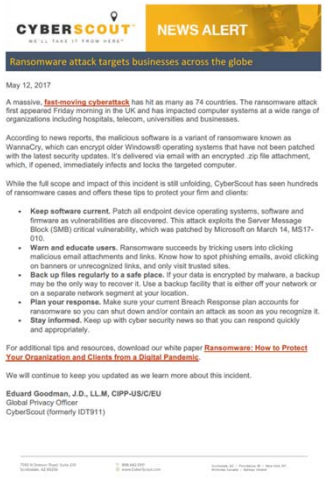
- Extortion threats
- Social engineering
- Cyber bullying
- Identity theft
- System compromise
- Internet cleanup

CYBERSCOUT

Example: WannaCry Ransomware Attack







CYBERSCOUT

Practice and Teach Good Cyber Hygiene

- Educate employees about cyber risks and the importance of reputation management.
  - Use caution when clicking on ads or links you receive in messages from friends.
  - Know what you've posted about yourself. Avoid sharing common security questions such as birthday, hometown, high school, father's middle name, current location.
  - Be selective about who you accept as a friend or connection on a social network.
  - Be careful when installing extras on your device or site such as third-party extensions and games.
  - Assume that everything you put on a social media site is permanent even if you delete it.

CYBERSCOUT

Engage to Learn and Communicate

Minimize	Monitor	Manage

• Educate on emerging risks
• Plan content around seasonal trends
  • Taxes, back-to-school, holiday
• Encourage regular feedback and engagement
• Survey customer needs and preferences
• Keep a regular cadence of communication
	• Respond in a timely manner
	• Demonstrate empathy
	• Route to the the appropriate person/department
	  • Is this a customer service issue?
	  • Is this a content issue?
	  • Is this a product issue?
	• Move the communication to a private channel
		• Initiate Crisis Response Plan
		• Communicate facts and what is known (avoid speculation)
		• Reinforce tips and education
		• Consider audiences not on social media / alternate channels
		  • Email, Newsletters, Hotline
		• Manage reputational damage and seek outside counsel/assistance
		• Evaluate the effectiveness of the response

CYBERSCOUT

46

Final Thoughts

- Cyber risks are beginning to outstrip traditional risks for businesses of all types and sizes -- now a global exposure.
- Regulators worldwide are focusing on consumer privacy in the digital realm.
- The insurance industry has stepped up to tackle the management of cyber risks and it's now spreading to all segments and lines.
- Insurance companies are at high risk of cyber exposures.
- You need an actively managed approach to risk management, response and remediation across the organization.
- Cyber risk = reputation management in the digital age -- if managed effectively, it can provide insurance companies with a market advantage.

CYBERSCOUT

47

Q

Any Questions?

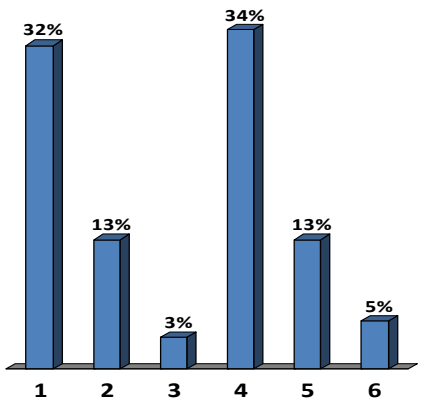
Matt Cullina | CEO
CyberScout
77 Eddy Street, 4th Floor
Providence, RI 02903

T: 401-680-4010
E: mcullina@CyberScout.com

CYBERSCOUT
WE'LL TAKE IT FROM HERE™

¿Cuán probable es que su empresa tenga un ciberataque significativo? How likely is your company to have a significant cyber attack?

1. **Ya ha sucedido** / *Has already happened*
2. **Muy poco probable** / *Very unlikely*
3. **Improbable** / *Unlikely*
4. **Probablemente** / *Likely*
5. **Muy probable** / *Very likely*
6. **No lo sé** / *I don't know*

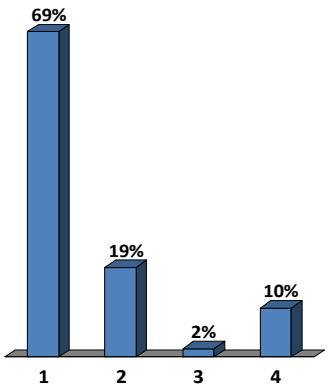


62

CYBERSCOUT

¿Su organización ha considerado ofrecer seguros cibernéticos a sus asegurados en líneas personales o comerciales?
Has your organization considered offering cyber insurance to either your personal or commercial lines policyholders?

1. **no estamos considerando** / not considering
2. **estamos investigando actualmente** / currently researching
3. **lanzaremos un seguro cibernético en 2018** / we will be launching cyber insurance in 2018
4. **ofrecemos seguros cibernéticos a nuestros asegurados** / we do offer cyber insurance to our policyholders

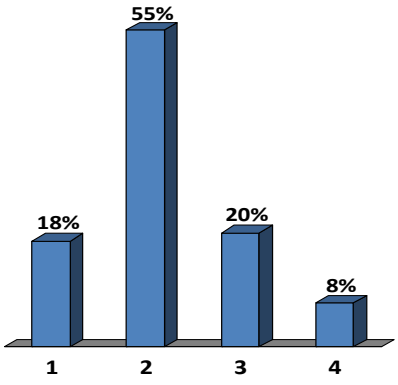


59

CYBERSCOUT

¿Como categorizaría la protección de su organización contra el riesgo cibernético?
How would you categorize your organization's protection against cyber risk?

1. **muy seguro** / *very secure*
2. **algo seguro** / *somewhat secure*
3. **no muy seguro** / *not very secure*
4. **no es seguro en absoluto** / *not secure at all*



66

CYBERSCOUT