



CYBER INSURANCE: A DEEP DIVE

Judy Selby
February 24, 2017

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

BDO[®]

**WITH YOU
TODAY**



JUDY SELBY
Managing Director
BDO Consulting
Technology Advisory Services

+1 203-905-6252 | jselby@bdo.com

AGENDA

- ▶ Today's Threat Landscape
- ▶ Understanding Your Risk
- ▶ Cybersecurity Risk Management Overview
- ▶ Cybersecurity Mitigation
- ▶ Cyber Insurance
- ▶ Conclusion

TODAY'S THREAT LANDSCAPE

CYBERSECURITY TODAY



TODAY'S THREAT LANDSCAPE

INTERNAL THREAT: Internal actors were responsible for 43% of data loss, half of which is intentional, half accidental.

COMPUTER INTRUSIONS: This year, companies that had data breaches involving less than 10,000 records, the average cost of data breach was \$4.9 million and those companies with the loss or theft of more than 50,000 records had a cost of data breach of \$13.1 million.

BUSINESS E-MAIL COMPROMISE: Between January 2015 and June 2016, there has been a 1,300% increase in identified exposed losses, a combined exposed dollar loss of more than \$3 billion.

RANSOMWARE: Nearly 80% of organizations [surveyed in the U.S.] have been victim of a cyber attack during the past 12 months and nearly 50% have been victim of a ransomware attack.

- Intel Security Report, Grand Theft Data: Data exfiltration study: Actors, tactics, and detection
- 2016 Data Breach Study: United States, Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, June 2016
- FBI Public Service Announcement, June 14, 2016; Alert Number I-061416-PSA
- Understanding the Depth of the Global Ransomware Problem, Osterman Research Survey Report, Published August 2016, Sponsored by Malwarebytes



TODAY'S THREAT LANDSCAPE

TODAY'S LANDSCAPE: DATA BREACHES BY THE NUMBERS

48%

caused by
malicious or
criminal attacks

\$4 million

average cost
of a data
breach

29%

increase in total
cost of data
breach since 2013

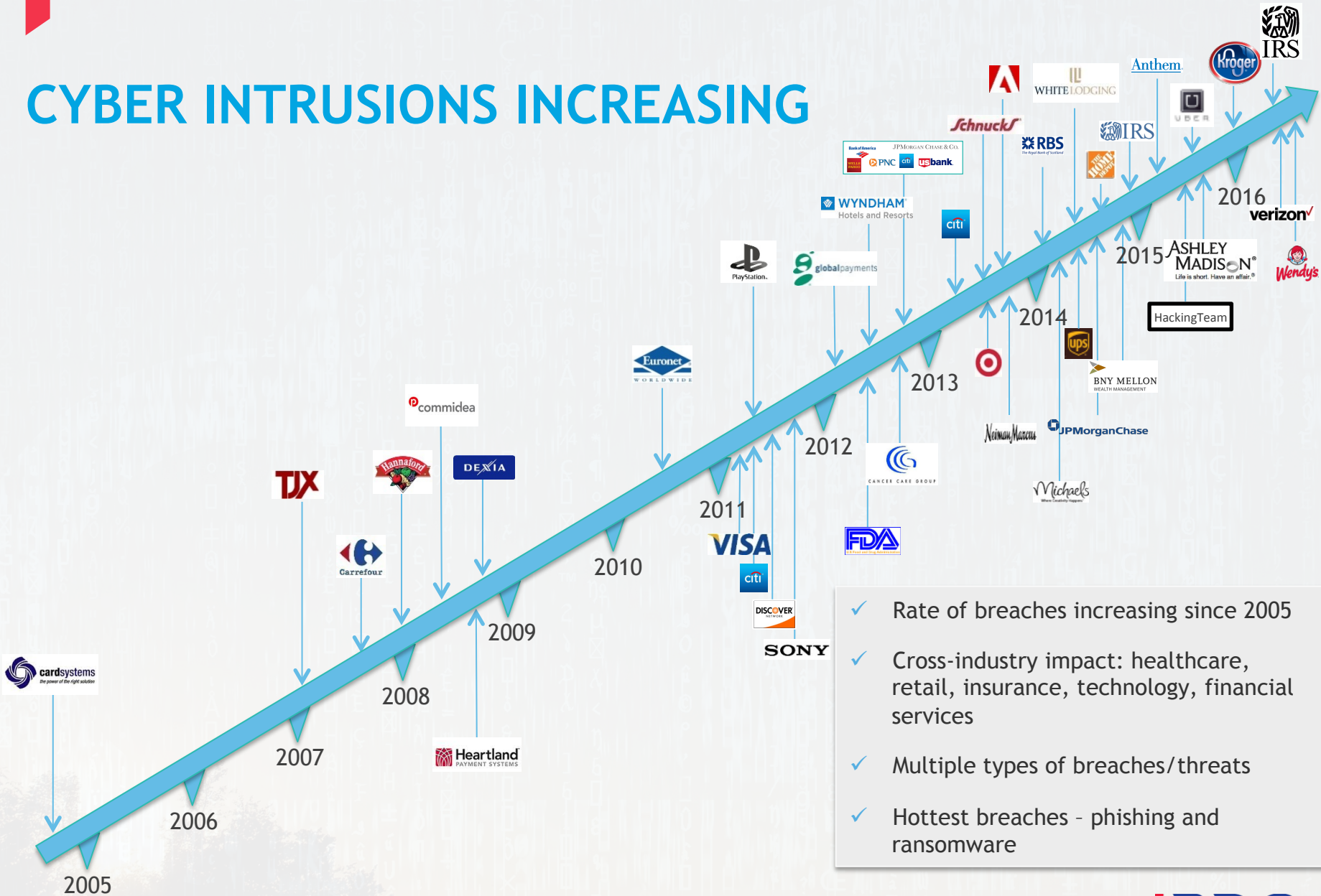
\$158

average cost per
lost or stolen
record

\$355

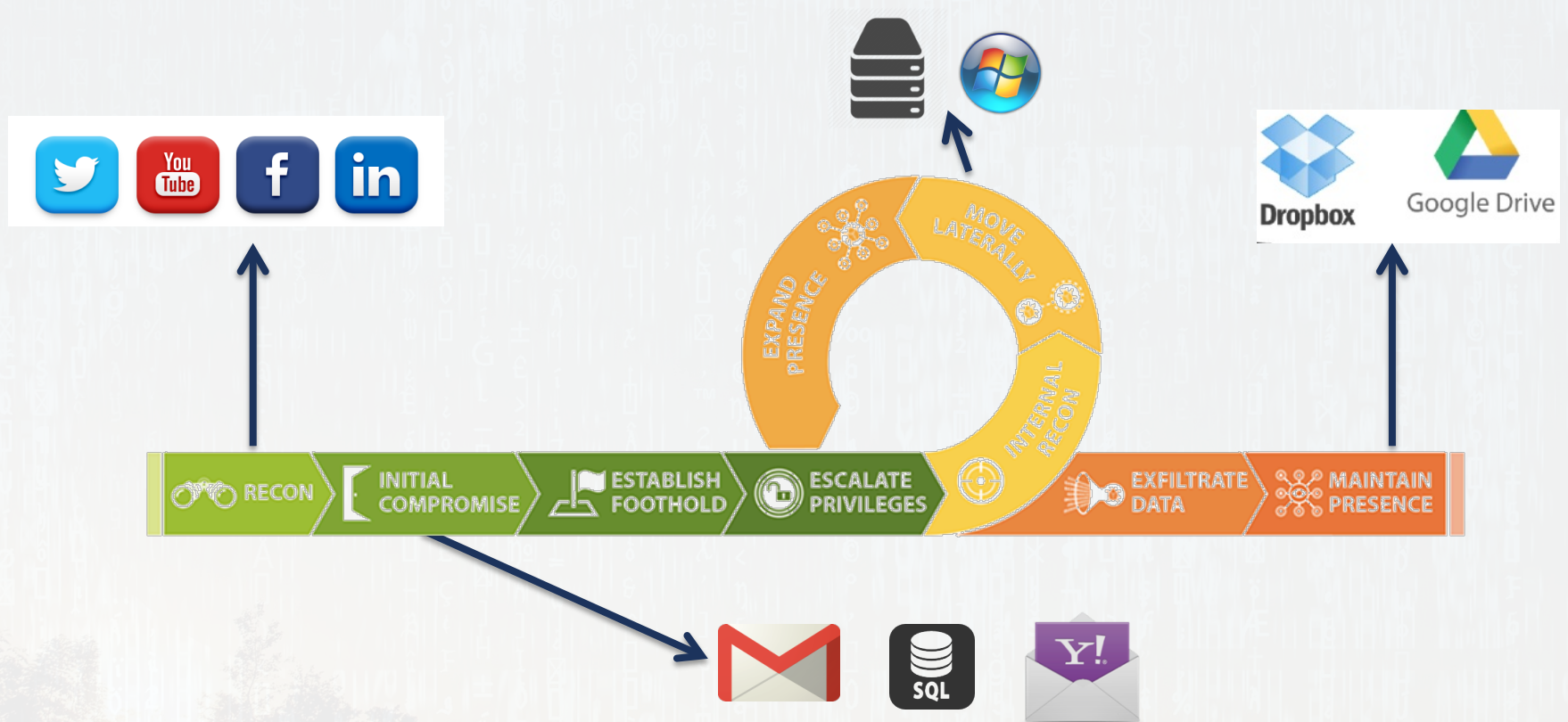
average cost per lost
or stolen record in
healthcare
organizations

CYBER INTRUSIONS INCREASING



- ✓ Rate of breaches increasing since 2005
- ✓ Cross-industry impact: healthcare, retail, insurance, technology, financial services
- ✓ Multiple types of breaches/threats
- ✓ Hottest breaches - phishing and ransomware

ANATOMY OF A HACK





UNDERSTANDING YOUR RISK



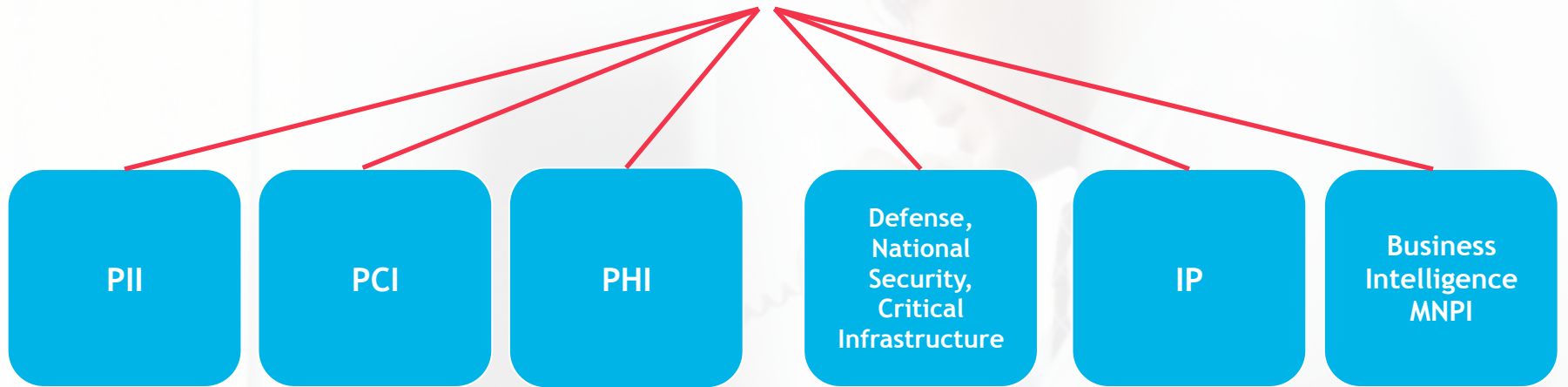
UNDERSTANDING YOUR RISK

THREAT
VULNERABILITY

+ CONSEQUENCE

RISK

TARGETED DATA











UNDERSTANDING YOUR RISK

LIFE CYCLE OF DATA PRIVACY AND PROTECTION



MOTIVATIONS AND INCENTIVES

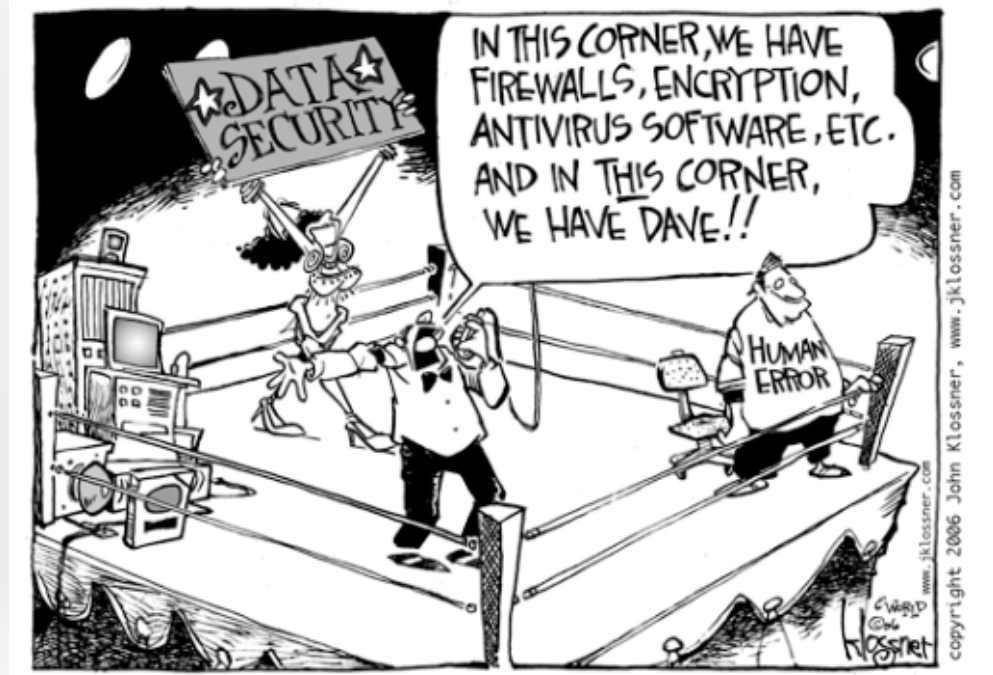
	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivist might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.



UNDERSTANDING YOUR RISK

EMPLOYEE RISKS

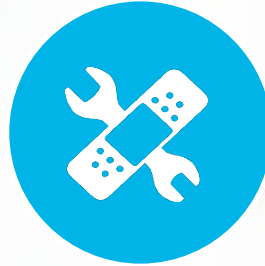
- ▶ **Employees as cyber targets**
 - ▶ Phishing
 - ▶ Spear Phishing / Social Engineering
 - ▶ Email spoofing and hijacking
- ▶ **Negligent Employees**
- ▶ **Non-compliant Employees**





UNDERSTANDING YOUR RISK

VULNERABILITIES



SOFTWARE PATCHING

Lack of software updates



ACCESS CONTROL

Who has access to your system and do they really need it?



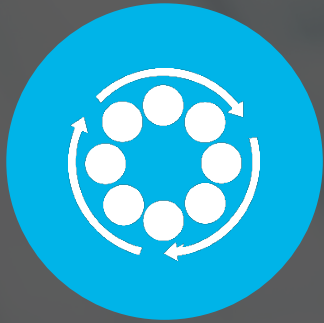
THIRD PARTY VENDORS

Are your third party vendors secure?



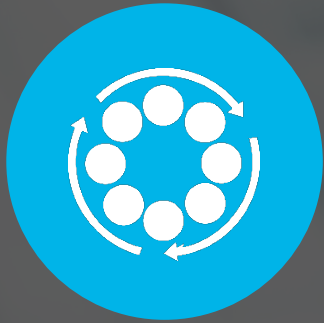
PEOPLE

Internal actors up to no good or being exploited



CYBERSECURITY RISK MANAGEMENT OVERVIEW

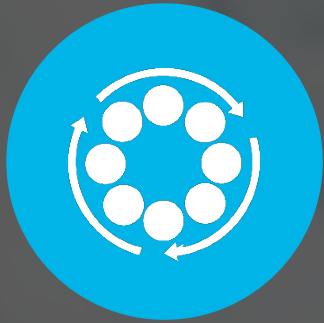




CYBERSECURITY RISK MANAGEMENT OVERVIEW

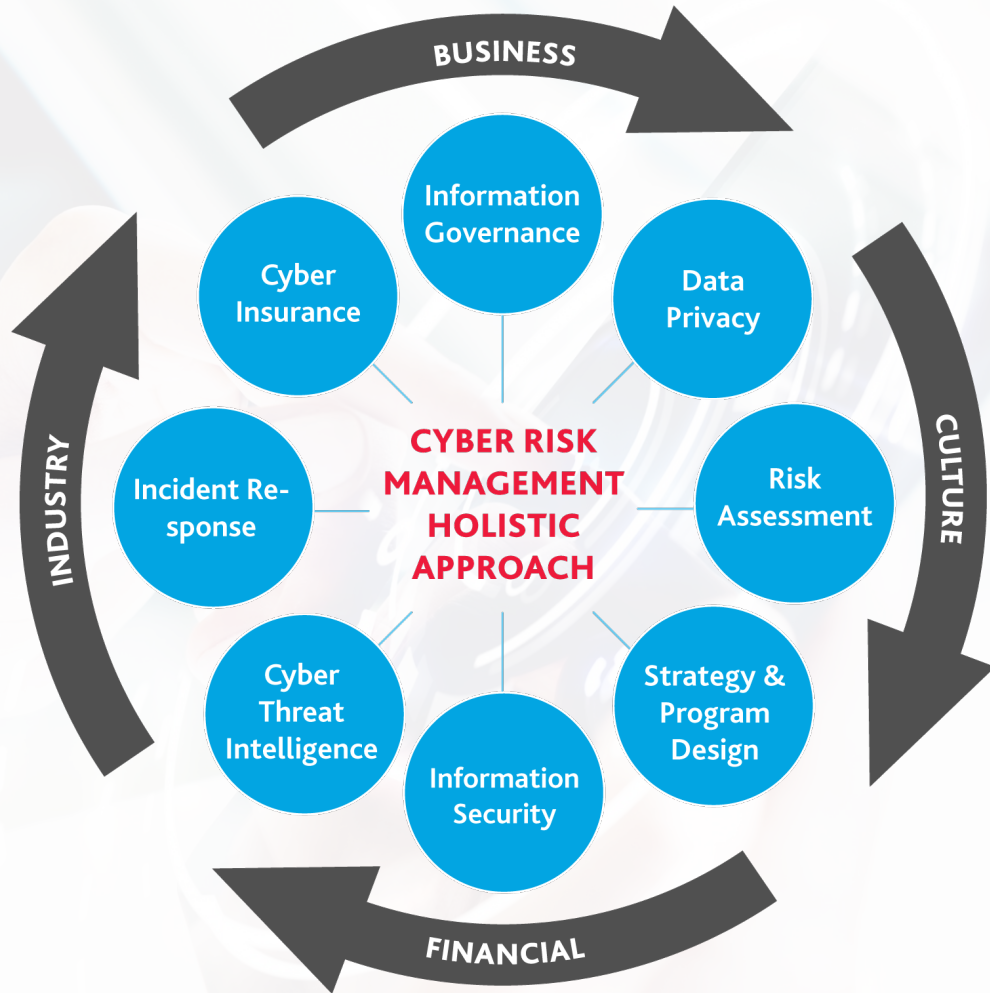
WHAT IS “CYBERSECURITY RISK MANAGEMENT PROGRAM”?

- ▶ **Integrated** set of policies, processes, technologies and controls that minimize vulnerabilities and protect against threat to support
- ▶ **Confidentiality** - information kept private and secure
- ▶ **Integrity** - data not inappropriately modified, deleted or added
- ▶ **Availability** - systems/information available to whom requires them



CYBERSECURITY RISK MANAGEMENT OVERVIEW

A HOLISTIC APPROACH





CYBERSECURITY MITIGATION

BDO CYBERSECURITY FRAMEWORK

Key Policy & Process Domains

- ▶ Data privacy / protection
- ▶ Identity & access management
- ▶ Threat & risk intelligence
- ▶ Third party / vendor management
- ▶ Incident response & planning
- ▶ Asset inventories
- ▶ Metrics / reporting
- ▶ Training / awareness

Cybersecurity Lifecycle



Governance & Strategy

- ▶ Cybersecurity risk profile management
- ▶ Cybersecurity risk management program
- ▶ Organization roles and responsibilities (Board of Directors, Executive Management, etc.)
- ▶ Investment optimization
- ▶ Legal & compliance
- ▶ Cyber insurance



CYBERSECURITY MITIGATION

THREAT INTELLIGENCE



Private Sector
Threat
Information



Government Classified
and Unclassified
Evidence and
Intelligence



Cyber Threat
Intelligence

INFORMATION SHARING CHANNELS



CYBERSECURITY MITIGATION





CYBER INSURANCE

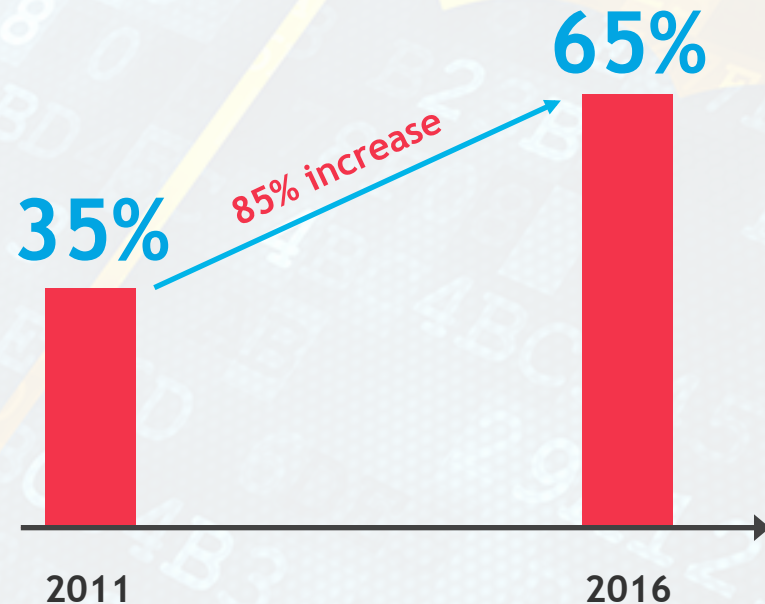




CYBER INSURANCE

THE GROWING CYBER INSURANCE MARKET

Proportion of companies buying
security & privacy insurance





CYBER INSURANCE

THE GROWING CYBER INSURANCE MARKET

View cyber risk as a significant threat



Purchase security & privacy insurance



SOURCE: https://www.zurichna.com/en/about/news/news-releases/2016/10272016_overall-upward-trend-continues-zurichs-advisen-cyber-survey

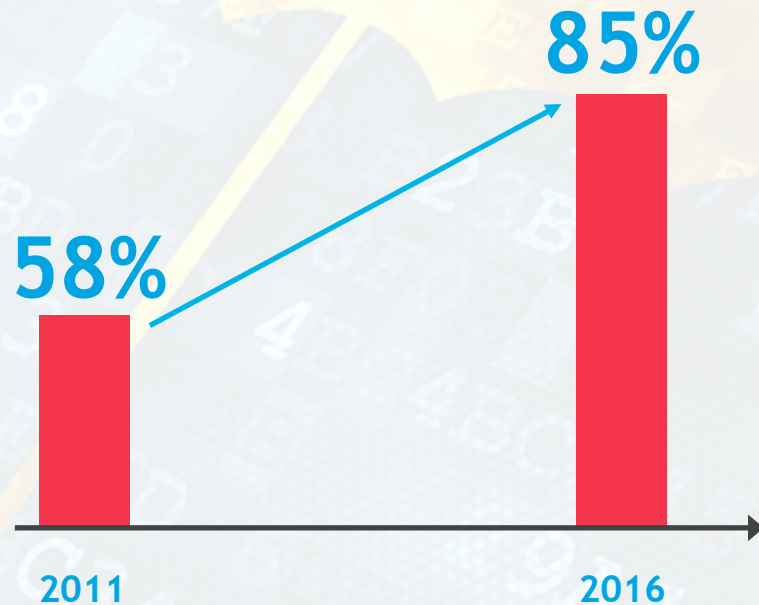




CYBER INSURANCE

THE GROWING CYBER INSURANCE MARKET

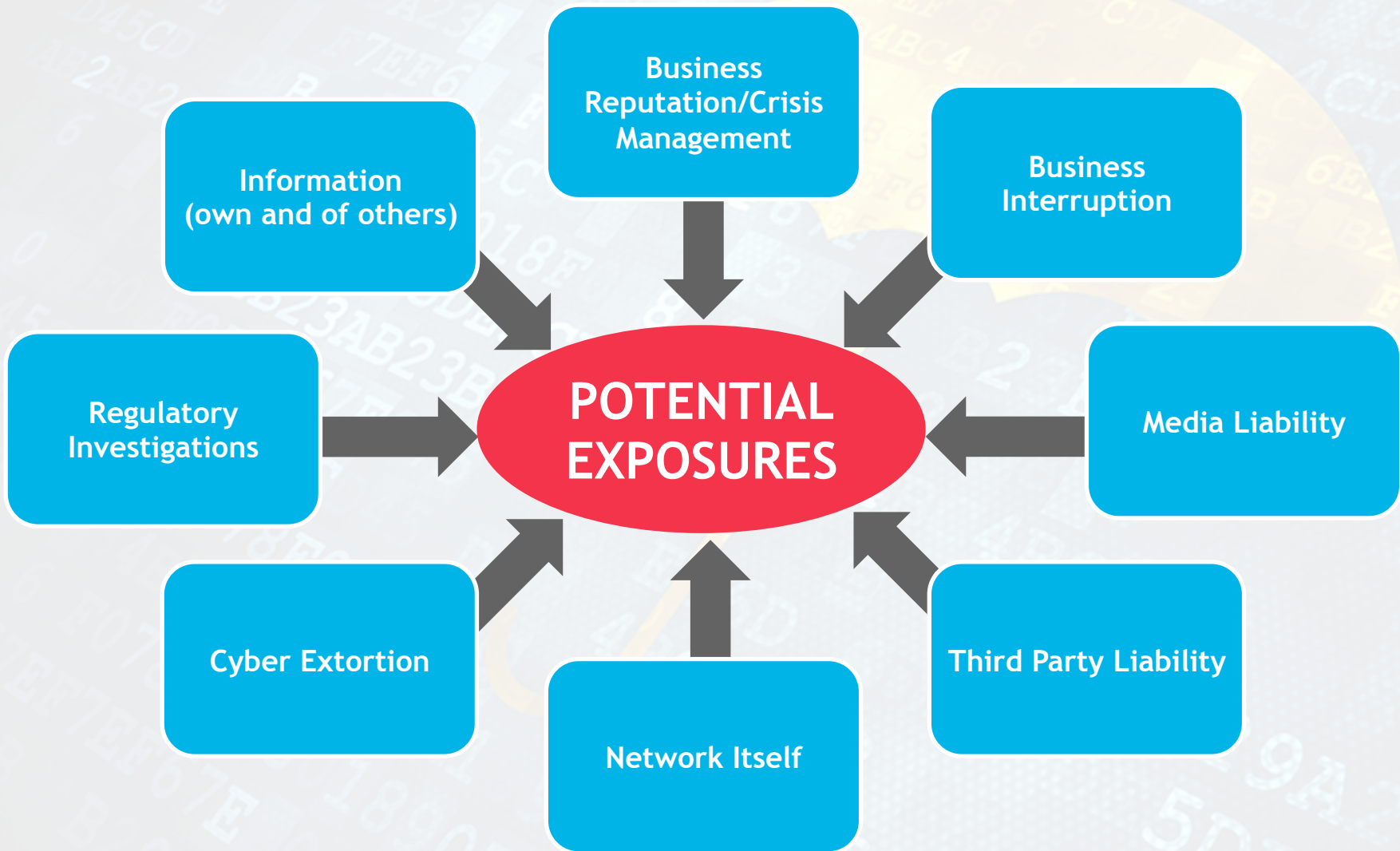
C-suite executives who view cyber security as a significant threat



21%

Have no employee
education program
in place







CYBER INSURANCE

INSURABLE CYBER RISKS

- ▶ Legal liability to others for computer security breaches
- ▶ Legal liability to others for breaches of confidential information
- ▶ Regulatory actions, fines and investigations
- ▶ Loss or damage to data and information
- ▶ Loss of revenue due to a computer attack
- ▶ Extra expense to recovery or respond to a computer attack
- ▶ Loss or damage to reputation
- ▶ Cyber-extortion
- ▶ Cyber-terrorism



CYBER INSURANCE

COVERAGE GRANTS

First Party

- ▶ Damage to digital assets
- ▶ Business interruption
- ▶ Extortion
- ▶ Privacy breach expenses

Third Party

- ▶ Privacy liability
- ▶ Network security liability
- ▶ Internet media liability
- ▶ Regulatory liability
- ▶ Contractual liability



CYBER INSURANCE

AVAILABLE COVERAGES

Network Security Liability

Liability to a third party as a result of a failure of your network security to protect against destruction, deletion, or corruption of a third party's electronic data, denial of service attacks against internet sites or computers; or transmission of viruses to third party computers and systems.

Privacy Liability

Liability to a third party as a result of the disclosure of confidential information collected or handled by you or under your care, custody or control. Includes coverage for your vicarious liability where a vendor loses information you had entrusted to them in the normal course of your business.



CYBER INSURANCE

AVAILABLE COVERAGES

Regulatory Investigative Defense

Coverage for legal expenses associated with representation in connection with a regulatory investigation, including indemnification of fines and penalties where insurable.

Event Response and Crisis Management Expense

Expenses incurred in response to a data breach event, including retaining forensic investigator, crisis management.

Cyber Extortion

Ransom and/or investigative expenses associated with a threat directed at you that would cause an otherwise covered event or loss.



CYBER INSURANCE

AVAILABLE COVERAGES

Network Business Interruption

Reimbursement of your loss of income and/or extra expense resulting from an interruption or suspension of computer systems due to a failure of technology. Includes coverage for dependent business interruption.

Data Asset Protection

Recovery of costs and expenses you incur to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed by a computer attack.



CYBER INSURANCE

UNDERWRITING FACTORS

- ▶ Industry
- ▶ Size of company
- ▶ Type and volume of data
- ▶ Risk management
- ▶ People
- ▶ Process
- ▶ Technology
- ▶ Incident response
- ▶ Claims



CYBER INSURANCE

COVERAGE DANGER ZONES

- ▶ Notice to the Insurer
- ▶ Retention of Counsel or Forensics Firm Before Notice
- ▶ Panel Firms?
- ▶ Pre-Notice Costs
- ▶ Effect of Breach Start Date
- ▶ Issues with Business Interruption Coverage
- ▶ Valuing a Cyber Claim
- ▶ Are the Limits Sufficient?



CYBER INSURANCE

PCI ISSUES

- ▶ Fines
- ▶ Penalties
- ▶ Assessments
- ▶ PFIs
- ▶ PCI Compliance Certifications
- ▶ PCI Recertification
- ▶ Affirmative Claims Against Processor, Card Brands, and QSAs
- ▶ Coverage for costs of responding to subpoenas or civil investigative demands



CYBER INSURANCE

NON-PII CYBER EVENTS

- ▶ Intellectual Property
- ▶ Proprietary and Confidential Business Information
- ▶ Bodily Injury
- ▶ Property Damage

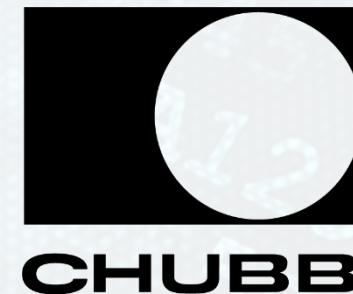


CYBER INSURANCE

EFFECTIVE INDEMNITY AGREEMENTS

Privacy Liability

“With respect to all Insuring Clauses, [Federal] shall not be liable for any Loss on account of any Claim, or for any Expense . . . based upon, arising from or in consequence of any . . . liability assumed by any Insured under any contract or agreement.”





CYBER INSURANCE

BUSINESS INTERRUPTION CONCERNS

With respect to the **NETWORK INTERRUPTION INSURING AGREEMENT** of this Clause 1., solely with respect to a Security Failure first occurring during the Policy Period and reported to the Insurer pursuant to the terms of this policy, this Network Interruption Coverage Section affords the following coverage:

NETWORK INTERRUPTION INSURING AGREEMENT

The Insurer shall pay all Loss in excess of the Remaining Retention that an Insured incurs after the Waiting Hours Period and solely as a result of a Security Failure.

(l) “Waiting Hours Period” means the number of hours set forth in Item 6 of the Declarations that must elapse once a Material Interruption has begun.



CYBER INSURANCE

HOW DO YOU SUBMIT A CLAIM?

- ▶ Documentation requirements
- ▶ Application of waiting periods/sub-limits (e.g., business interruption versus network interruption)
- ▶ Common items of dispute in the adjustment process





CONCLUSION



OUR CYBERSECURITY SERVICES

- ▶ Cyber Risk Management Strategy & Program Design
- ▶ Cyber Risk Assessment & Security Testing
- ▶ Data Privacy & Protection
- ▶ Security Architecture & Transformation
- ▶ Incident Response Planning
- ▶ Business Continuity Planning & Disaster Recovery
- ▶ Digital Forensics & Cyber Investigations
- ▶ Cyber Insurance Claim Preparation & Coverage Adequacy Evaluation



SPEAKER BIO



JUDY SELBY

Managing Director
BDO Consulting
Technology Advisory Services

+1 203-905-6252

jselby@bdo.com

Judy Selby is a Managing Director in BDO Consulting's Technology Advisory Services practice, having more than 20 years of experience in insurance and technology. Known as "one of the premier voices in legal technology" by *Legaltech News*, she consults with clients on cyber insurance, cybersecurity, information governance, data privacy and complex insurance matters. She advises clients on best practices for handling information throughout its life cycle, from creation or collection through disposition.

In addition, Judy works with organizations and their counsel to advise on data privacy and cyber insurance issues, having depth of experience in coverage adequacy evaluation, international arbitration and all phases of insurance coverage litigation.

Prior to joining BDO, Judy was a partner at Baker Hostetler, where she was co-chair of the Information Governance team and founder of the eDiscovery and Technology team. She is the co-chair of the Claims and Litigation Management (CLM) Alliance Cyber Liability Committee and serves on the Law360 Insurance and Legaltech News editorial boards. Judy has completed courses on the internet of things (IoT), big data, crisis management / business continuity and cybersecurity at the Massachusetts Institute of Technology.



About BDO Consulting

BDO Consulting, a division of BDO USA, LLP, provides clients with Financial Advisory, Business Advisory and Technology Services in the U.S. and around the world, leveraging BDO's global network of more than 64,000 professionals. Having a depth of industry expertise, we provide rapid, strategic guidance in the most challenging of environments to achieve exceptional client service.

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your firm's individual needs.

© 2016 BDO USA, LLP. All rights reserved.