PLUS

PROFESSIONAL LIABILITY UNDERWRITING SOCIETY

Cyber Liability

Threats, Coverage, and Surviving a Breach

Panelists

- Kirstin Simonson: 2nd Vice President, Travelers
  - Global Technology Cyber Leader
- Mario Paez: Vice President, Wells Fargo Insurance
  - National Practice Cyber Advisor
- Mark Lanterman: Chief Technology Officer, Computer Forensic Services

PLUS

Agenda

- Cyber Event Case Study
- Evolution of Cyber Liability Exposures
- Gap Analysis: Traditional Policy Deficiencies
- Insurance Solutions
- Cyber Event Response
- Underwriting Implications

PLUS

Cyber Event Case Study

PLUS

Cyber Event Case Study

Cyber Event Case Study

Fraudulent Wire

- $952,800 wire
- Romania
- RSA token
- Bookkeeper- denies involvement

Cyber Event Case Study

Analysis

- Evidence is consistent
- Zeus

Cyber Event Case Study

Dear Mr. Caravello Chief Financial Officer - CFO ,

Winfield Community Bank , 27w111 Geneva Rd

The Federal Deposit Insurance Corporation (FDIC) has to report that counterfeit cashier's checks

The counterfeit items display a large variaty of routing numbers, which are assigned to a large numbe
to small and medium size banks all over USA. The items are blue, have rounded corners, and display
security feature statement embedded within a darkened top border. The bank's logo, name, and Web
site address appear near the top-left corner of the counterfeit items.
Authentic cashier's checks are yellow and display a security padlock icon at the end of the written
dollar amount line. The b n the top-center area.

http://sysfrb.org/check.fraud/oct2011.asp
Click to follow link

Copies of a counterfeit ite en at
https://fdic.gov/starsmail/check.sample.asp for your your review.

11034, Arlington, Virginia 22226, or transmitted electronically to alert@fdic.gov. Questions related to federal deposit insurance or consumer issues should be submitted to the FDIC using an online form that can be accessed at http://www2.fdic.gov/starsmail/index.asp

For your reference, FDIC Special Alerts may be accessed from the FDIC's Web site at www.fdic.gov/news/news/SpecialAlert/2011/index.html .
To learn how to automatically receive FDIC Special Alerts through e-mail, please visit www.fdic.gov/about/subscriptions/index.html

Sandra L. Thompson
Director
Division of Risk Management Supervision
Attachment (not available electronically)

Cyber Event Case Study

Ukrainian General Arrested in Cyber Heists

80 tweets retweet

A decorated Ukrainian general was arrested last week in Romania along with two other men suspected of being part of an organized cybercrime gang that laundered at least $1.4 million stolen from U.S. and Italian firms.

Apprehended in Iasi, Romania last week were **Matei Vitalie**, 37, of Moldova; **Konstantin Ossipov**, a 42-year-old Israeli citizen; and 54-year-old **Valeriu Gaichuk**, a Ukrainian general who, according to his Facebook page, once studied at Florida International University in Miami.

Gen. Valeriu Gaichuck, far right.

Romanian prosecutors allege that the men created fake companies and business contracts to help to launder funds that were stolen from at least two firms, including $952,800 from the **Society of Corporate Compliance and Ethics**, an organization based

Evolution of Cyber Liability: Insurance and Exposures

- Late 1990's
  - With evolution of technology, started to see insurance evolving to address
  - Early policies focused on media/content exposures
- Early 2000's
  - Online media policies began starting to cover liability associated with data breach and virus transmission
  - Several exclusions
  - California Security Breach and Information Act became effective
- Mid 2000's
  - Started to see 1st party coverages
- 2010's
  - Number of carriers with a standalone cyber policy exploded
  - 2014 – Year of the Retail Breach
  - 2015 – Year of the Healthcare Breach
  - 2016 – Continued evolution of insurance response

Evolution of Cyber Liability: Insurance and Exposures

Threat Actors

- Payment cards
- Credentials
- Bank account info

- Credentials
- Internal organization data
- Trade secrets
- System information

- Politically or socially motivated
- System disruption
- Internal organization data

Evolution of Cyber Liability: Insurance and Exposures

Legal Issues and Regulatory Environment

Legally mandated

- 47 states with privacy breach notification laws
  - Recent federal executive orders – will federal legislation finally be passed? Will it preempt?
- HIPAA/HITECH regulations
- FTC
  - Federal Trade Commission Act Section 5, Red Flags
- State Consumer Protection Laws
  - California's Song-Beverly Credit Card Act
- Foreign laws and regulations
  - EU Privacy Directive – Broader than US laws
- Other federal laws
  - SEC Guidance, COPPA, FCRA, FACTA, etc.

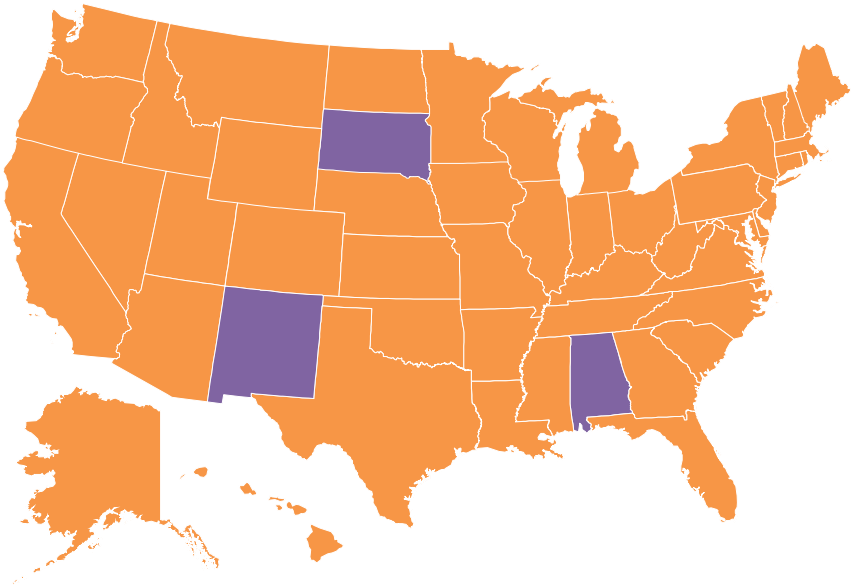
Industry Standard

- PCI DSS compliance
  - Required if storing, processing or transmitting payment card data
  - Significant fines, penalties and costs assessed
- Contractual obligations
  - Increasingly included in insurance provisions of customer/vendor contracts

Evolution of Cyber Liability: Insurance and Exposures

State Regulations: Notice Requirements

•47 states and 4 U.S. jurisdictions require notice to customers after unauthorized access to PII



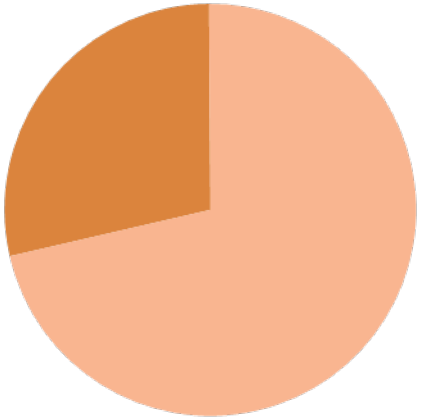
- Timing requirements for notifying residents
  - "without unreasonable delay" (means not later than 30 days)
  - FL was 45, is now 30 days
- Notify State Attorneys General, consumer protection agencies and credit reporting agencies
  - New requirement in ND, OR, and FL
- Timing requirements for notifying regulators and credit reporting agencies
  - 48 hours; 14 days; before notice to residents
- Constant Change - Amendments bring changes in MT, NV, ND, OR, TN, UT, VA, WA, WY, LA, IO, CT
  - Broader definitions of Personal Information and new protections for student data
  - More specific content in notice letters
  - CT to be first state to require by law that credit monitoring be provided

PLUS

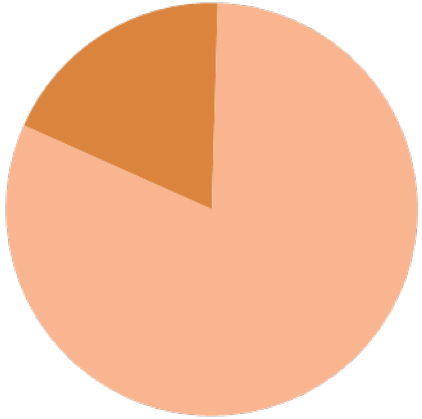
Evolution of Cyber Liability: Insurance and Exposures

2015 Data Breach Threats

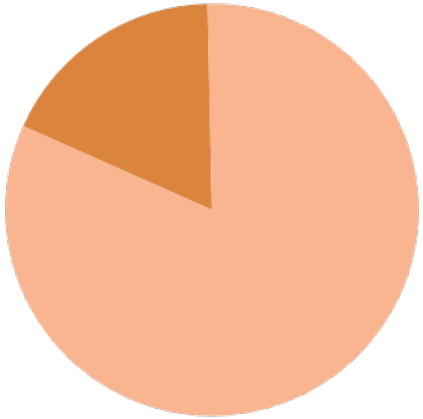
28.5%
POS Intrusions



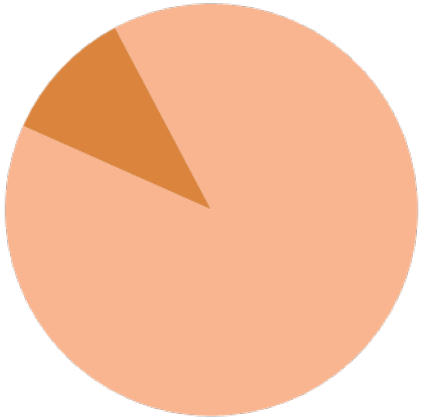
18.8%
Crimeware



18%
Cyber Espionage



10.6%
Insider Misuse



2,122 confirmed data breaches
(up from 1,367 in 2014)

79,790 reported security incidents
(up from 63,437 in 2014)

61 countries represented
(down from 95 in 2014)

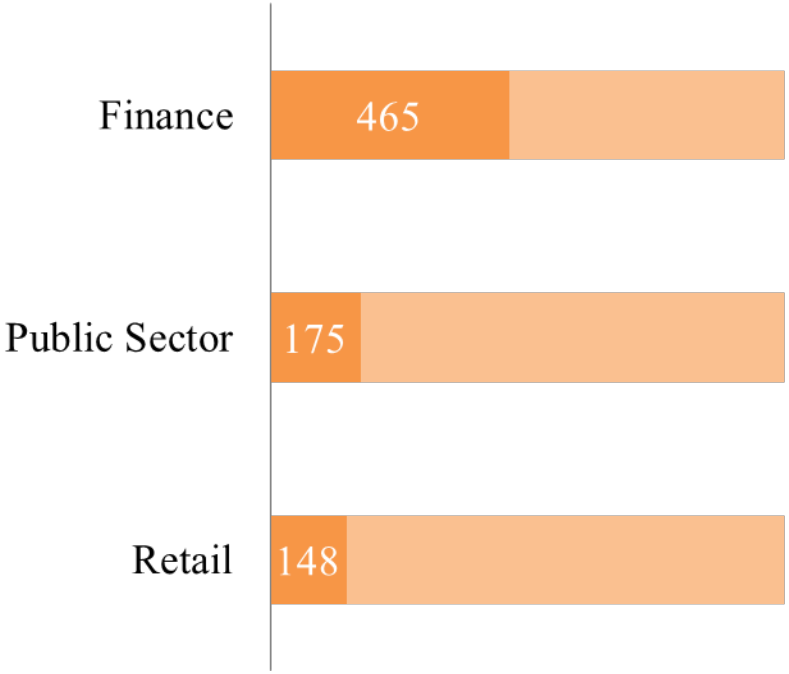
Verizon: 2015 Data Breach Investigations Report

PLUS

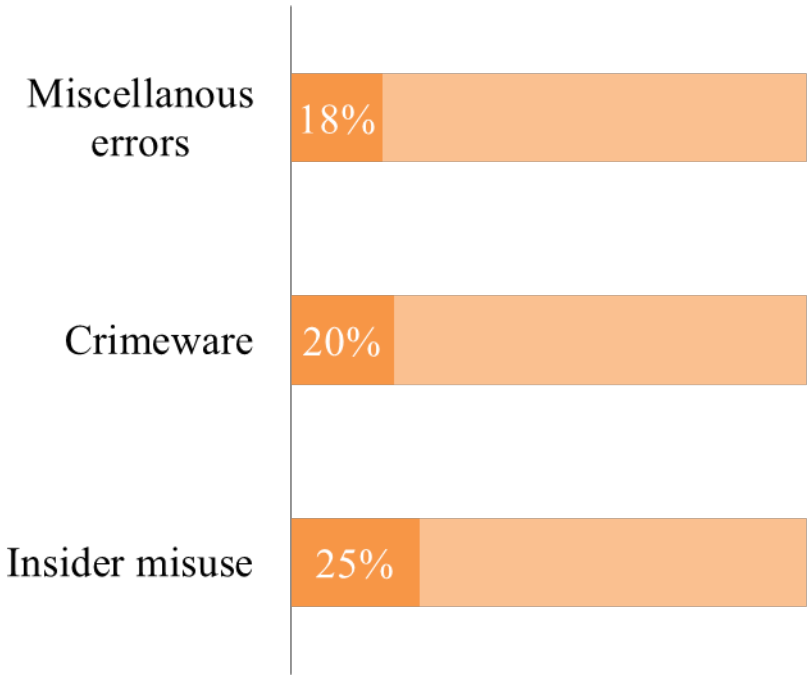
Evolution of Cyber Liability: Insurance and Exposures

2015 Confirmed Data Breaches By Industry

2,122 Confirmed Breaches – Top 3 Industry Classes



79,790 Incidents – How did they occur?



Verizon: 2015 Data Breach Investigations Report using 50 contributing global organizations.

Evolution of Cyber Liability: Insurance and Exposures

2015 Claims Study: Preliminary Findings

Data type	Cause of loss	Business sectors
• PII - 45% • PHI - 27% • PCI - 14%	• Hackers - 31% • Malware/virus - 14% • Staff mistakes and rogue employees tied – 11%* *First time rogue employees in top 3 causes	• Healthcare sector - 21% • Financial services - 17% • Retail – 13%* *Largest breaches occurred in retail

Data

•Sample size – 160 insured claims
•PII data type in 2014 study – 41%
•PCI data type in 2014 study – 19%
•PHI data type in 2014 study – 21%

Company size

•Nano-cap (under $50 million in revenue) experienced the most incidents – 29%
•Small-cap (under $2B in revenue) followed closely at 25%

Cyber Risk Claims: A Review of Industry Losses Paid Out - NetDilligence® 2015 Study

PLUS

Gap Analysis: Traditional Policy Deficiencies

	Property	General Liability	Crime	K&R	E&O	Cyber
1st Party Exposure/Loss						
Physical damage to data only		x		x		✓
Virus/hacker damage to data only		x	x	x		✓
Denial of service (DOS) attack		x	x	x		✓
Business interruption loss from security event		x	x	x	x	✓
Extortion or threat	x	x	x	✓	x	✓
Employee sabotage of data only	x	x		x		✓
Impostor fraud	x	x		x	x	
3rd Party Exposure/Loss						
Theft/disclosure of private information	x		x	x		✓
Confidential corporate information breach	x		x	x		✓
Technology E&O	x	x	x	x	✓	x
Media liability (electronic content)	x		x	x		✓
Privacy breach expense and notification	x	x	x	x		✓
Damage to 3rd party's data only	x			x		✓
Regulatory privacy defense / fines	x	x	x	x		✓
Virus/malicious code transmission	x		x	x		✓

x - No Coverage - Possible Coverage ✓ - Coverage

PLUS

Insurance Solutions

First Party	May include expenses paid to Insured for: • Data breach notifications and related expenses • Forensics and legal services • Extortion demands, including ransomware • Business interruption loss • Data Restoration costs • Credit or identity monitoring expense
Third Party	May include liability coverage for: • Data breach or other information security breaches • Intellectual property/media/content offenses • Regulatory defense and associated fines/penalties • PCI DSS contract penalties assessment defense • Professional services/E&O liability

PLUS

Cyber Event Response

PLUS

Underwriting Implications

- Exposure Evaluation
  - Critical risk analysis
    - Data breach = records
    - Business Interruption = lost profits due to inability to conduct business
    - Liability = professional exposures
    - Intellectual property = content
- Management Controls
  - Formalized, tested and monitored
    - Network and Information Security = Incident Response Plan
    - Business Interruption = Business continuity plan, including testing of backups
    - Intellectual Property = IP Clearance and due diligence