What is a breach?

What is a privacy breach / security breach?

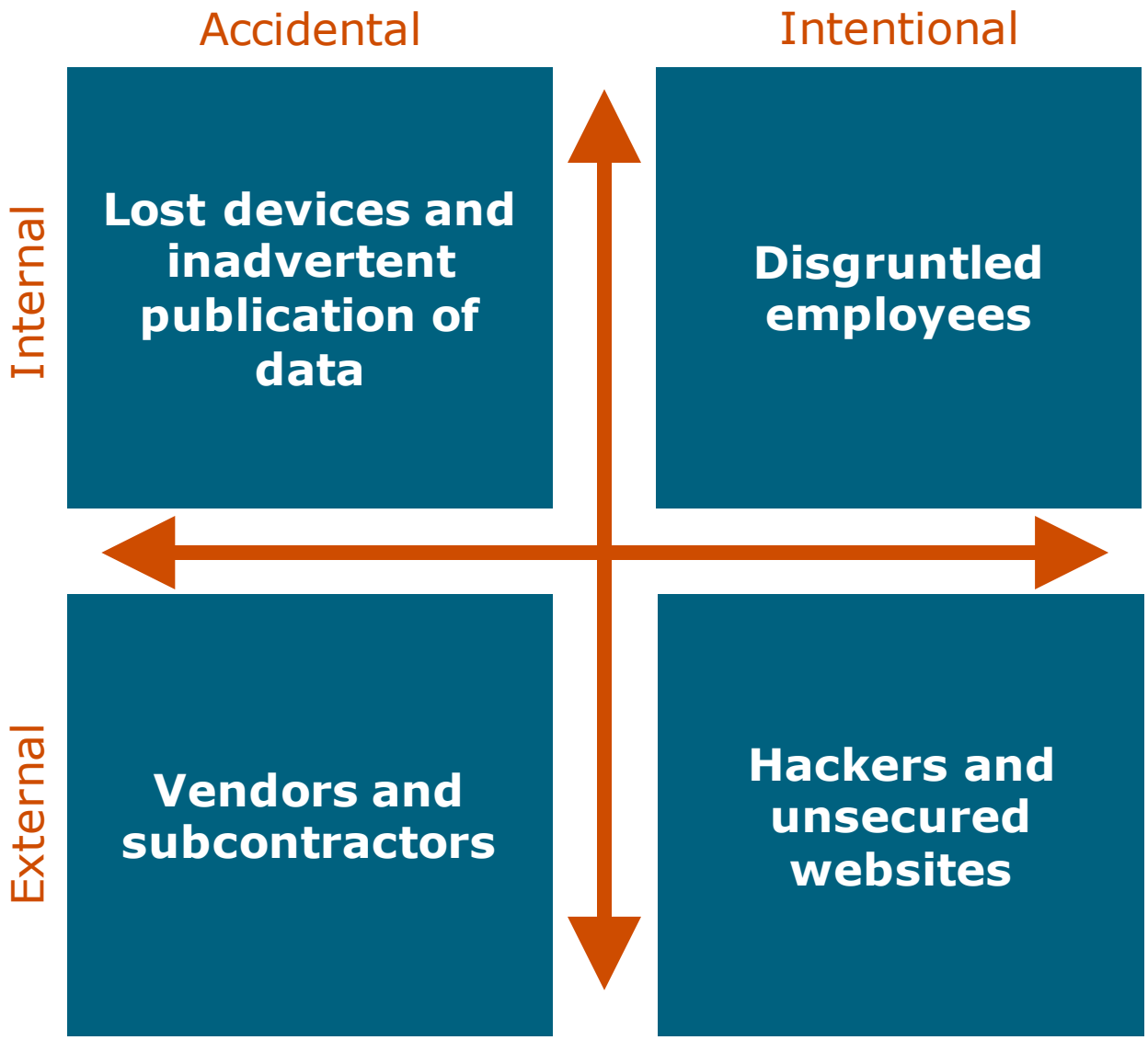
Privacy breach

The theft, loss or unauthorized disclosure of personally identifiable non-public information (PII) or third party corporate confidential information that is in the care, custody or control of the organization or an agent or independent contractor that is handling, processing, sorting or transferring such information on behalf of the Organization.

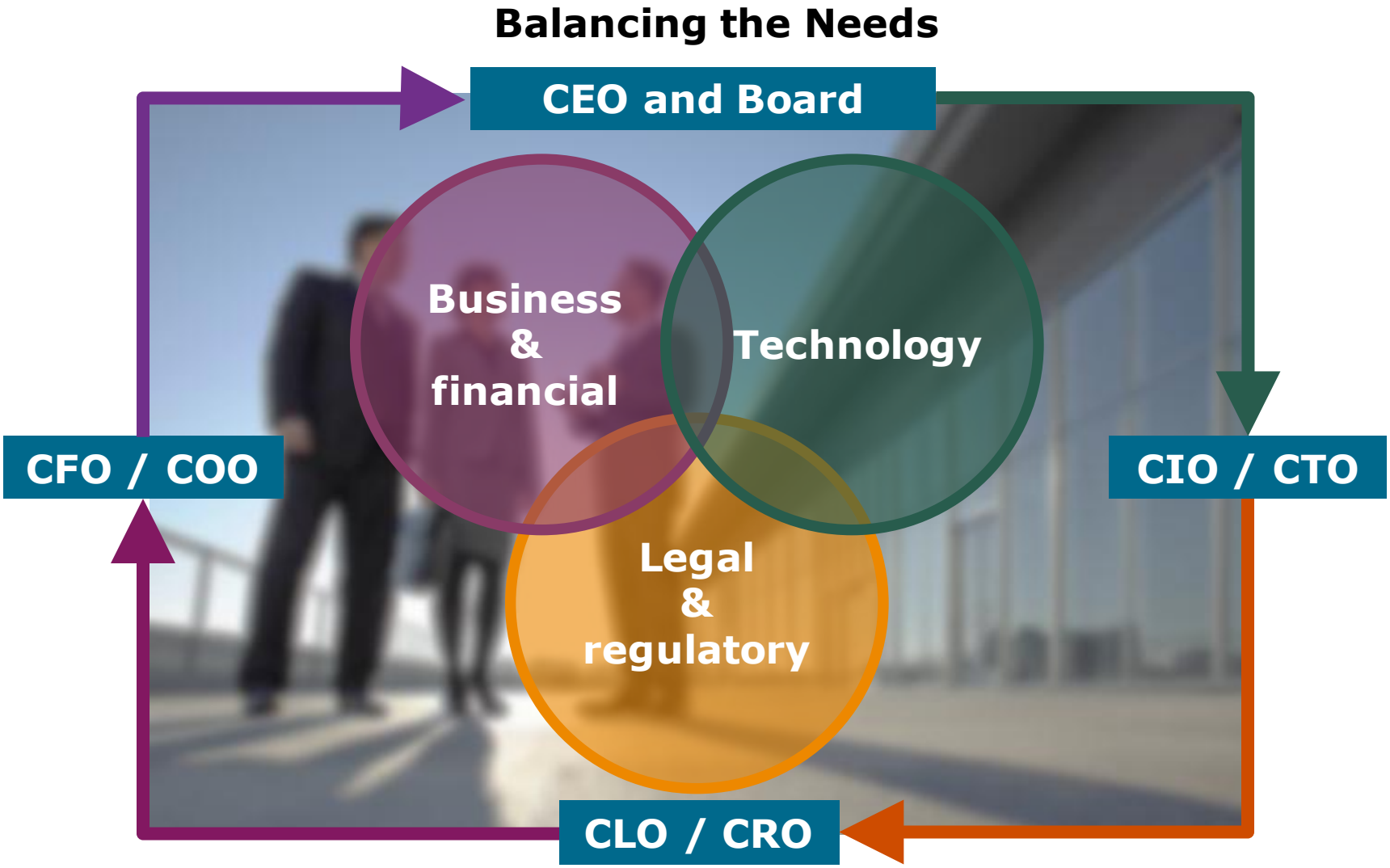
Computer security breach:

- The inability of a third party, who is authorized to do so, to gain access to an organization's systems or services;
- The failure to prevent unauthorized access to an organization's computer systems that results in deletion, corruption or theft of data;
- A denial of service attack against an organization's internet sites or computer systems; or
- The failure to prevent transmission of malicious code from an organization's systems to a third party computers and/or systems.

How do data breaches occur?



The C-Suite

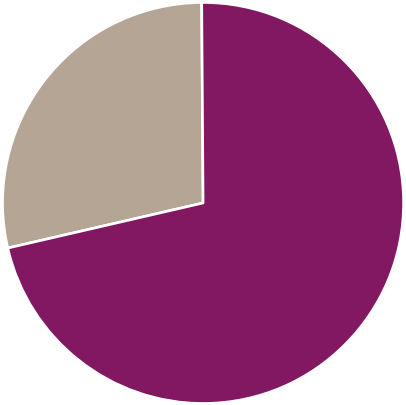

Balancing the Needs
CEO and Board
Business & financial
Technology
CFO / COO
CIO / CTO
Legal & regulatory
CLO / CRO

Statistics

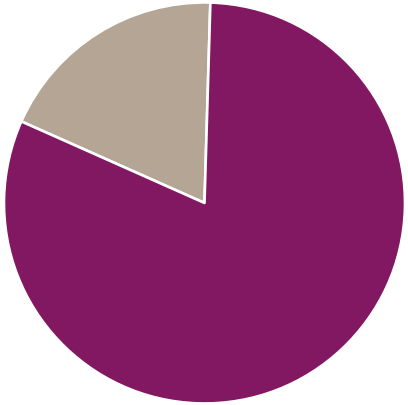
Verizon 2015 data breach investigations report

By the numbers

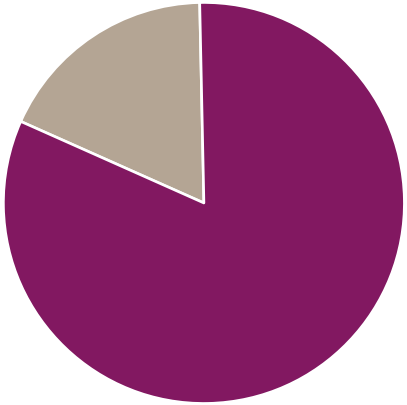
28.5% POS intrusions



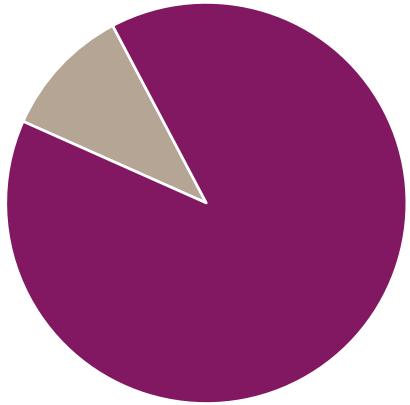
18.8% crimeware



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)

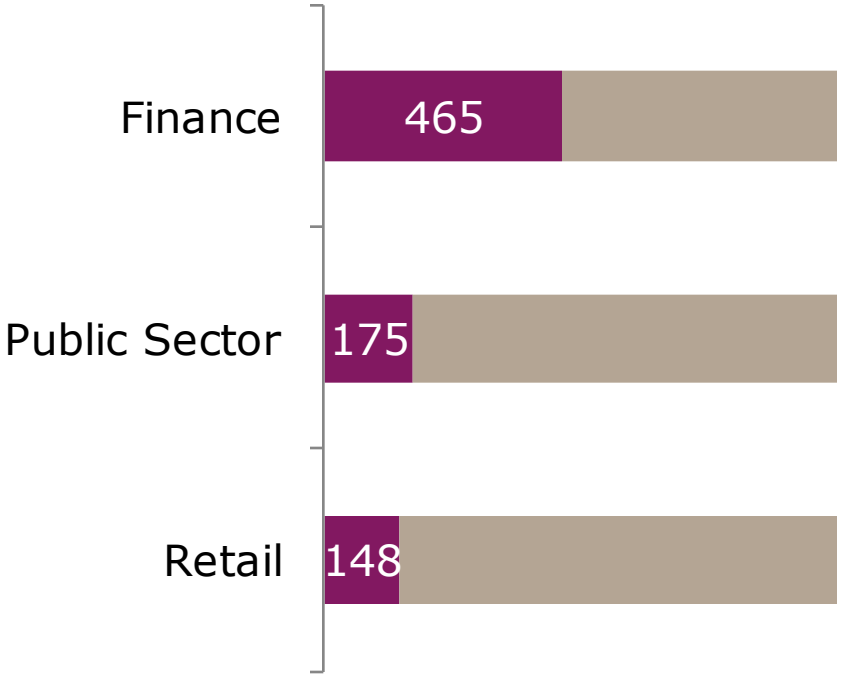
61 countries represented
(down from 95 in 2015)

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

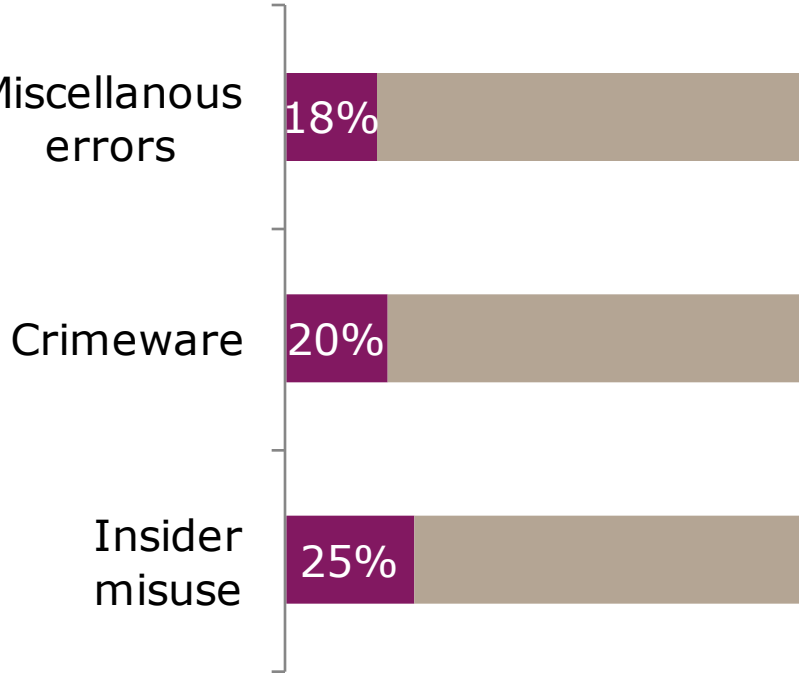
Verizon 2015 data breach investigations report

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.

NetDiligence 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

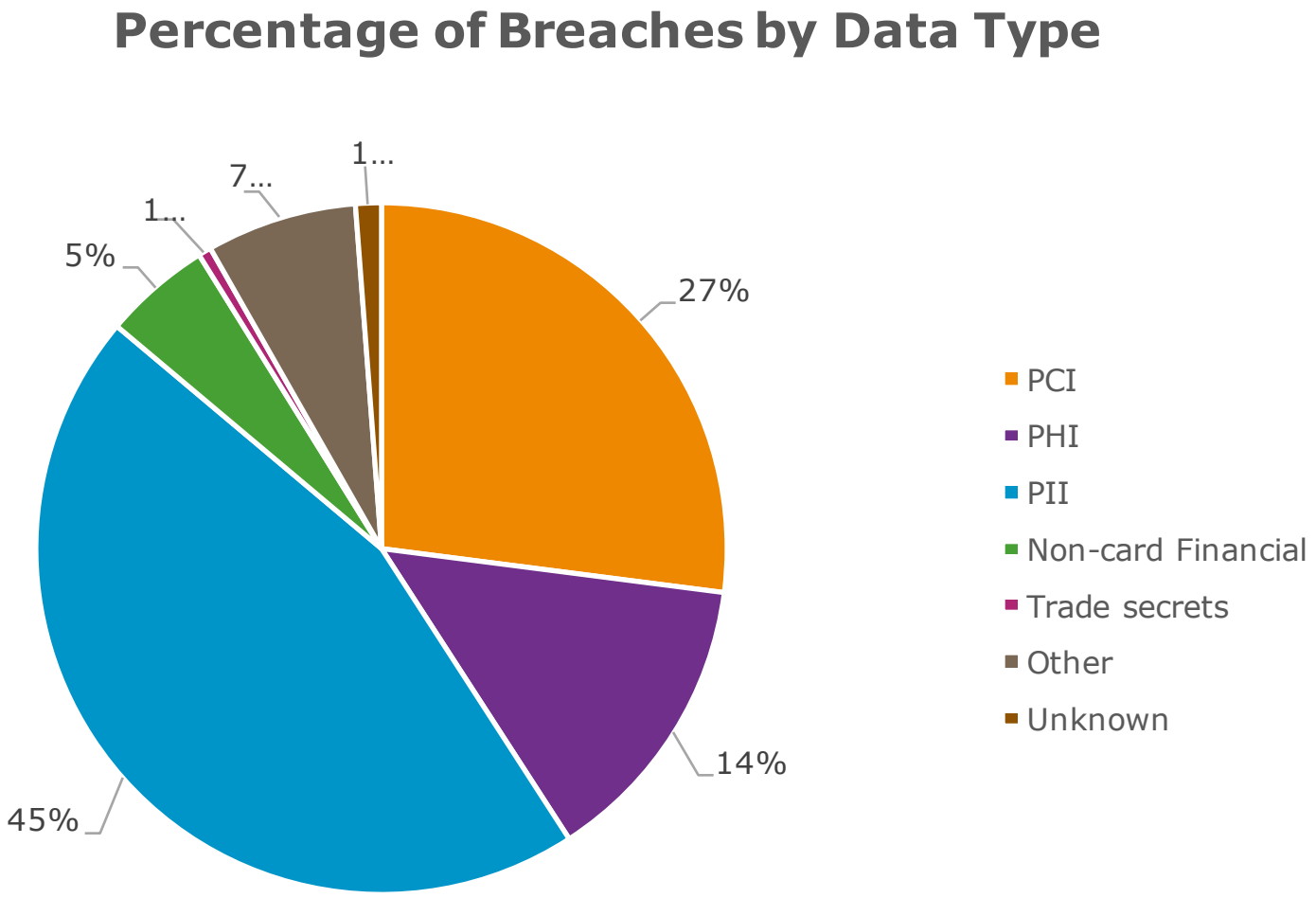
- Sample size – 160 insured claims
- PII data type in 2014 study – 41%
- PCI data type in 2014 study – 19%
- PHI data type in 2014 study – 21%

Company size

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

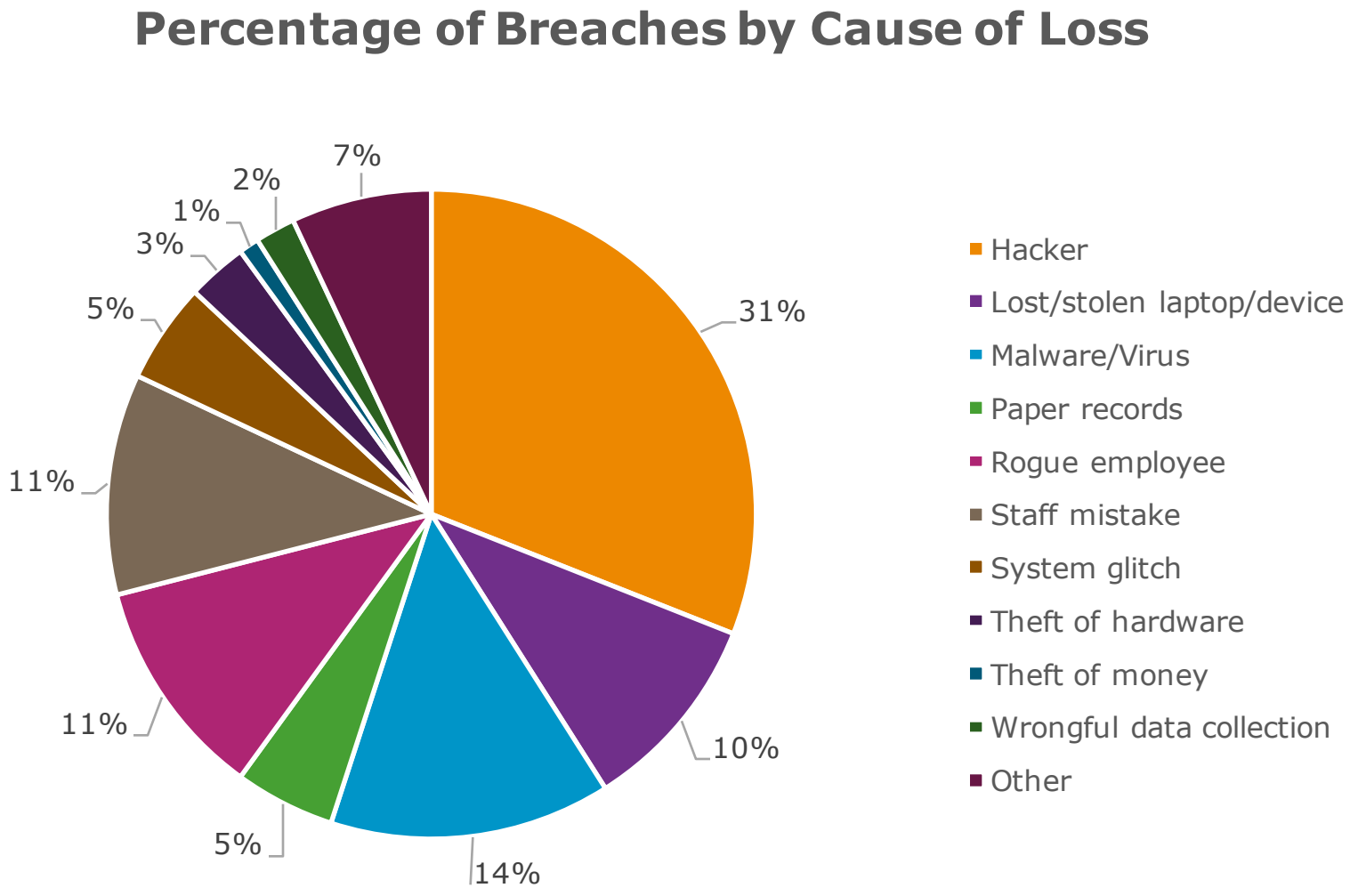
Cyber Risk Claims: A Review of Industry Losses Paid Out - NetDilligence® 20145Study (Sample size = 160 insured claims)

NetDiligence 2015 claims study



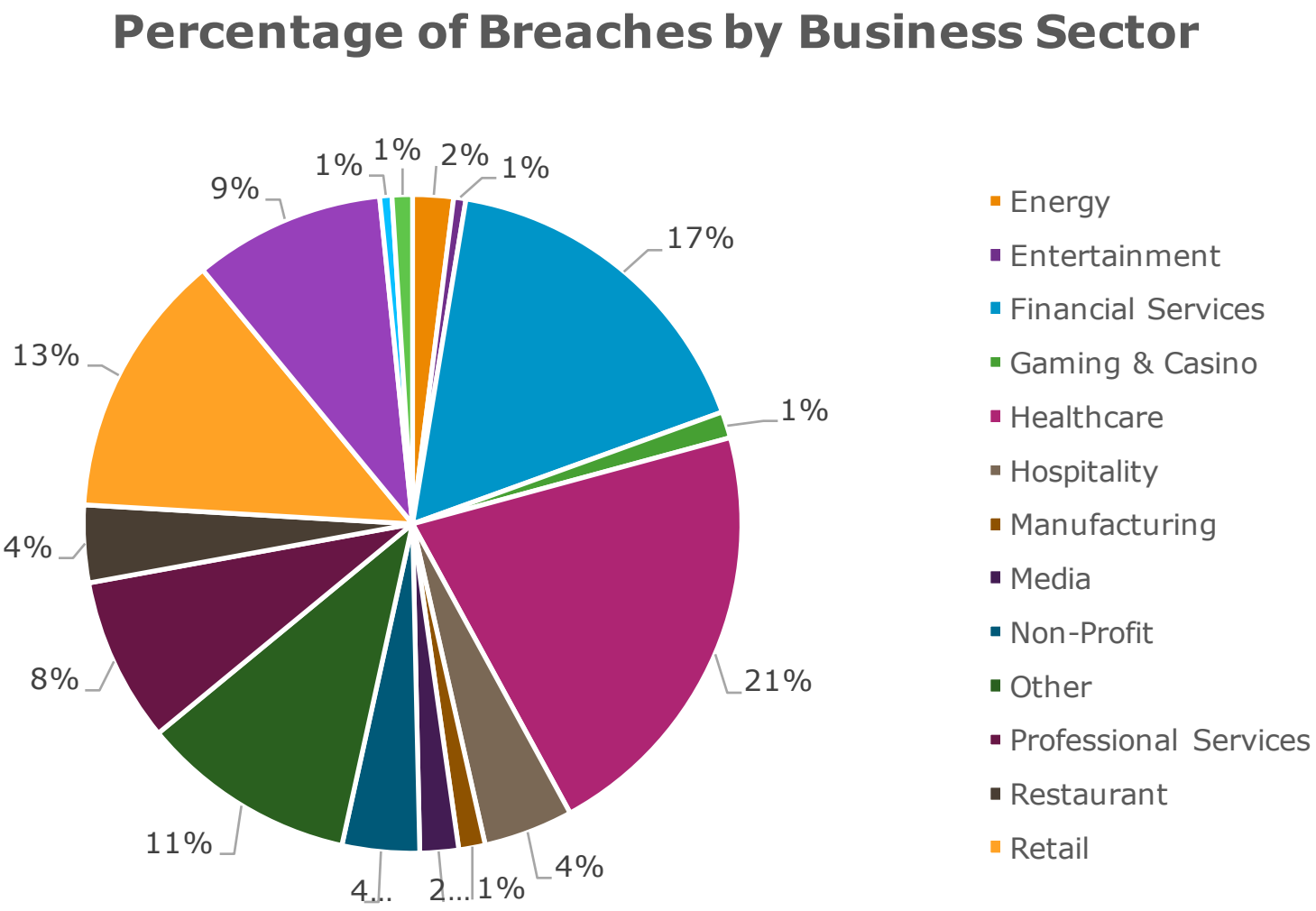
NetDiligence® 2015 Cyber Claims Study (Sample size = 160 insured claims)

NetDiligence 2015 claims study



NetDiligence® 2015 Cyber Claims Study (Sample size = 160 insured claims)

NetDiligence 2015 claims study



NetDiligence® 2015 Cyber Claims Study (Sample size = 160 insured claims)

Changes in the landscape.....

Neiman Marcus

7th Circuit Court of Appeals

"Customers should not have to wait until hackers commit identify theft or credit card fraud in order to be given standing because there is an 'objectively reasonable likelihood' that such an injury will occur."

Coca-Cola

The theft of encrypted laptops (55) by a former employee resulted in the breach of approximately 74,000 employee records

Eastern District of Pennsylvania found that "Here, plaintiffs' harm are not 'future harms' but ongoing, present, distinct and palpable harms" and allowed the allegations of breach of express and implied contract and unjust enrichment to survive.

Wyndham

"Wyndham Ruling Boost FTC's Authority to Investigate Security Breaches"

Wyndham is now under increased scrutiny by the FTC for 20 years and must follow strict data privacy requirements.

Concentra

"Concentra, HCA Health Plan HIPAA Settlements Emphasize HHS' Focus on Breach Risks Relating to Unencrypted Laptops"

$1.7 million fine plus $250,000 to resolve OCR investigation.

Grander scheme of things

A security event can have severely negative impact on your reputation and it could:

- Adversely impact your debt covenants
- Impair cash flow as funds are redirected to respond to the costs associated with the security event
- Affect your credit rating
- Redirect the focus of key employees from their daily jobs (the estimated "people-hour" cost for a breach is $30 per record breached)
- Cause an exodus of customers
- Create vulnerabilities that competitors can exploit

Current Regulatory and Legal Environment

Legal issues and the regulatory environment

Legally mandated

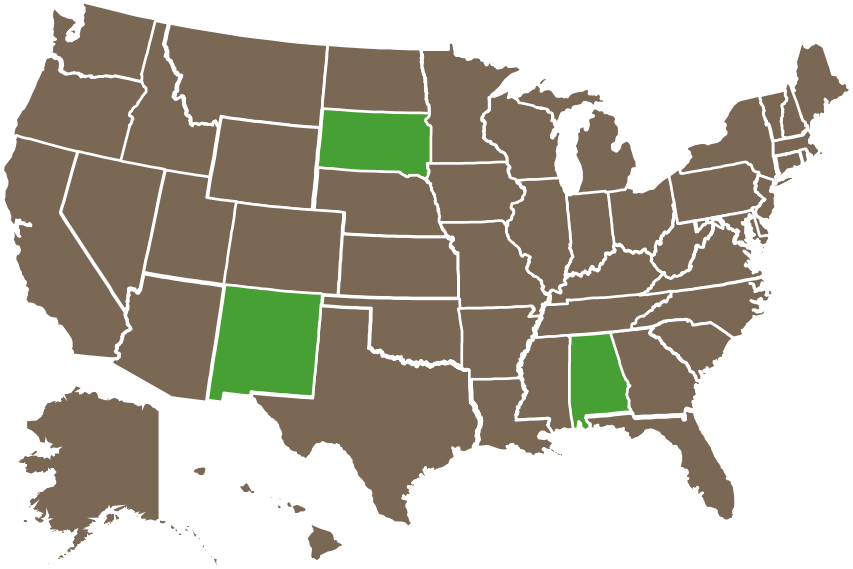
- 47 states with privacy breach notification laws
  - Recent federal executive orders – will federal legislation finally be passed? Will it preempt?
- HIPAA/HITECH regulations
- FTC
  - Federal Trade Commission Act Section 5, Red Flags
- State Consumer Protection Laws
  - California's Song-Beverly Credit 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

State regulations: notice

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; fourteen 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

Network Security & Privacy Insurance

Network security and privacy insurance

- Continue to see insurers grow their loss prevention and loss mitigation services for midsize companies.
- Network security risk is not going away.
- For any market that has pulled capacity, or has been hesitant to enter, another has stepped in.
- Most organizations are looking to transfer the risk to an insurance product.
- Cyber insurance market to reach $5 billion in written premium by 2020

Network security and privacy GAP analysis

	Property	General Liability	Crime	K&R	E&O	Network Security & Privacy
1st Party Privacy / Network Risks						
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 Privacy / Network Risks						
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

Network security and privacy liability

Combines:

- Third party liability
- First party reimbursement insurance
- First party business interruption and data asset loss

Different names depending on who you talk to…
Cyber Risk, Cyber Security, Data Security, Privacy Liability, Security Liability, Network Risk, etc.
They all essentially refer to the same thing.

Over 30+ markets with primary policy forms — which carriers will be around 5 years from now?

Insurance solutions

Third party liability coverage

- Privacy liability
- Network security
- Media liability
- Regulatory action* (sub-limit may apply)

Regulatory expenses, notification expenses, credit monitoring and other crisis management expenses are generally offered on a sub-limited basis and varies by carrier.

First party reimbursement coverage

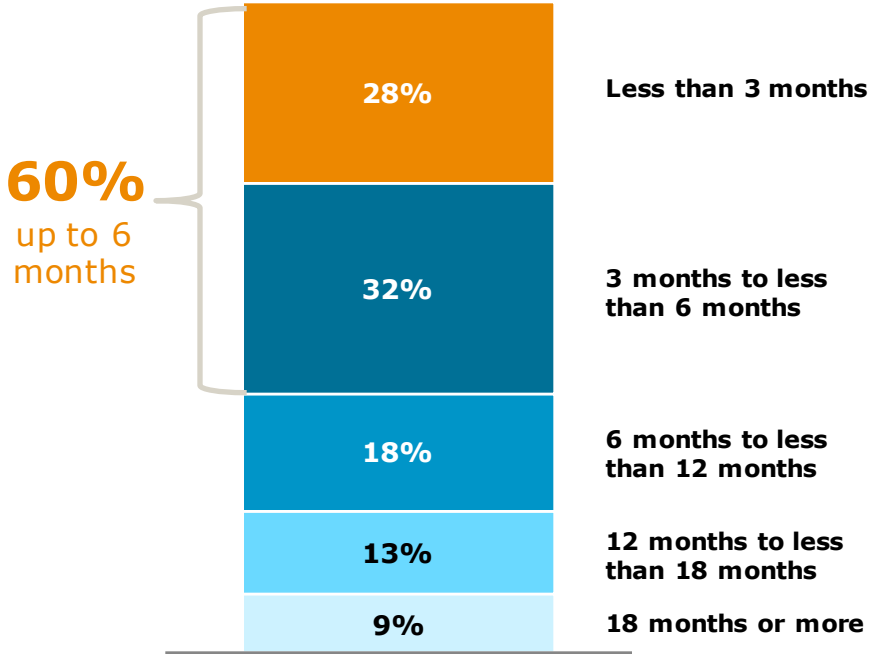
- Privacy notification costs
- Crisis management expenses
- Credit monitoring costs
- Forensic investigation

Other first party reimbursement coverages

- Cyber extortion
- Business interruption
- Data restoration

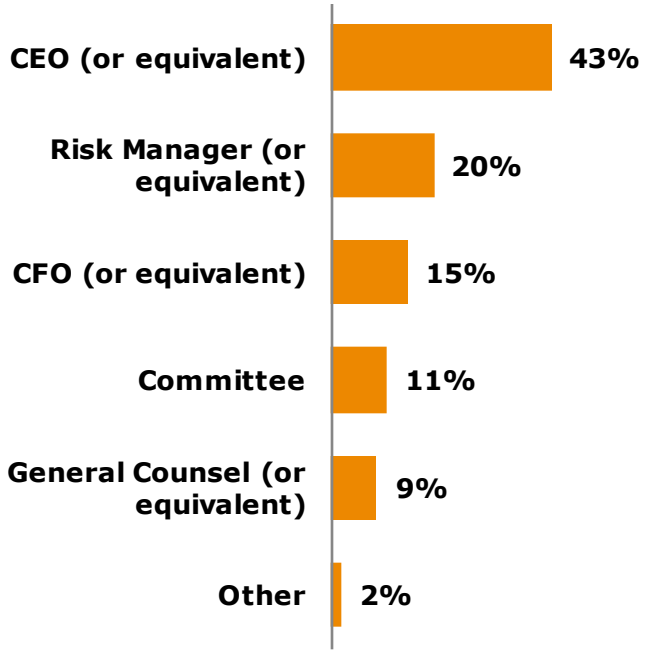
2015 Wells Fargo Insurance study

Decision time for cyber and data privacy insurance purchase



Base: Purchases cyber and data privacy insurance (n=84)

Decision-maker for purchase

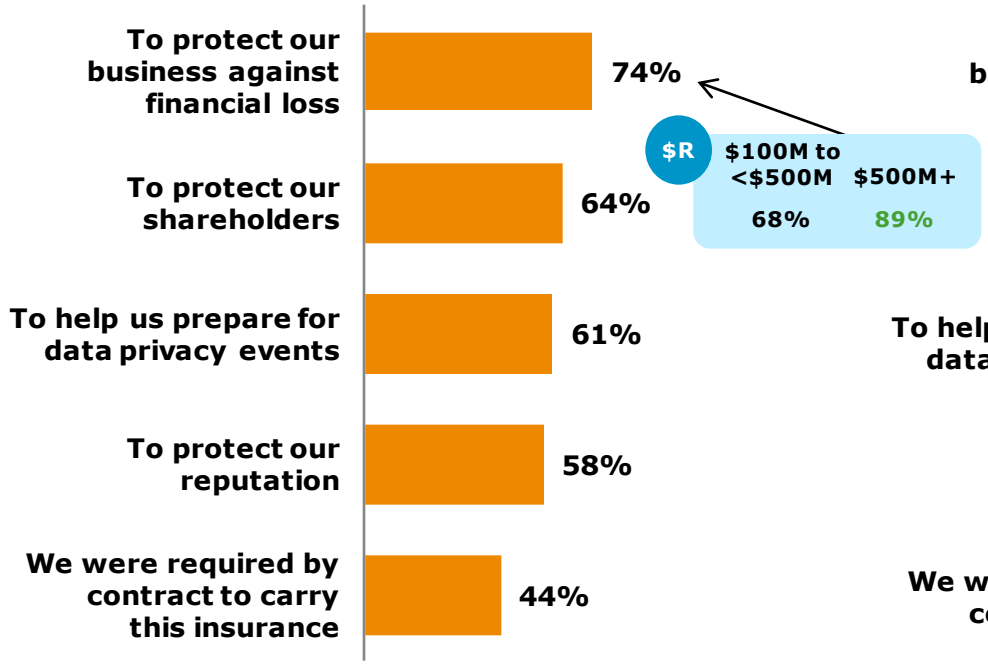


Base: Purchases cyber and data privacy insurance (n=84)

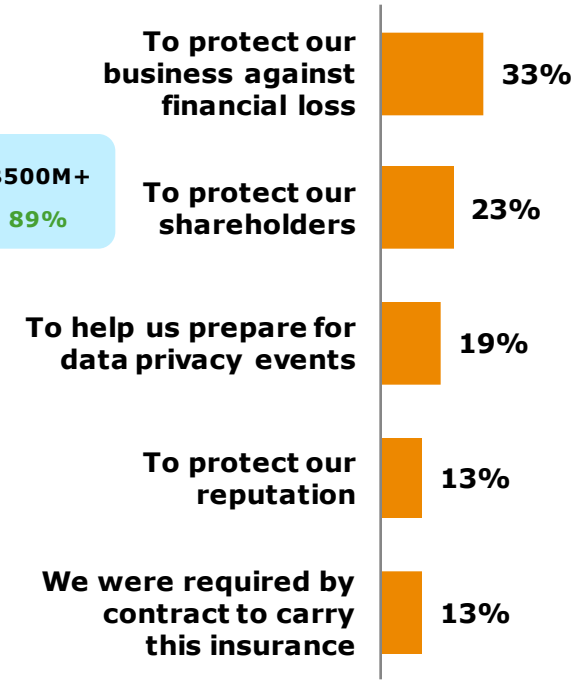
- Q.A3: Who ultimately decided to purchase cyber and data privacy risk insurance?
- Q.A2: How long did it take to make the decision to purchase cyber and data privacy risk insurance?

2015 Wells Fargo Insurance study

Reasons for purchasing cyber and data privacy insurance



Most important reason

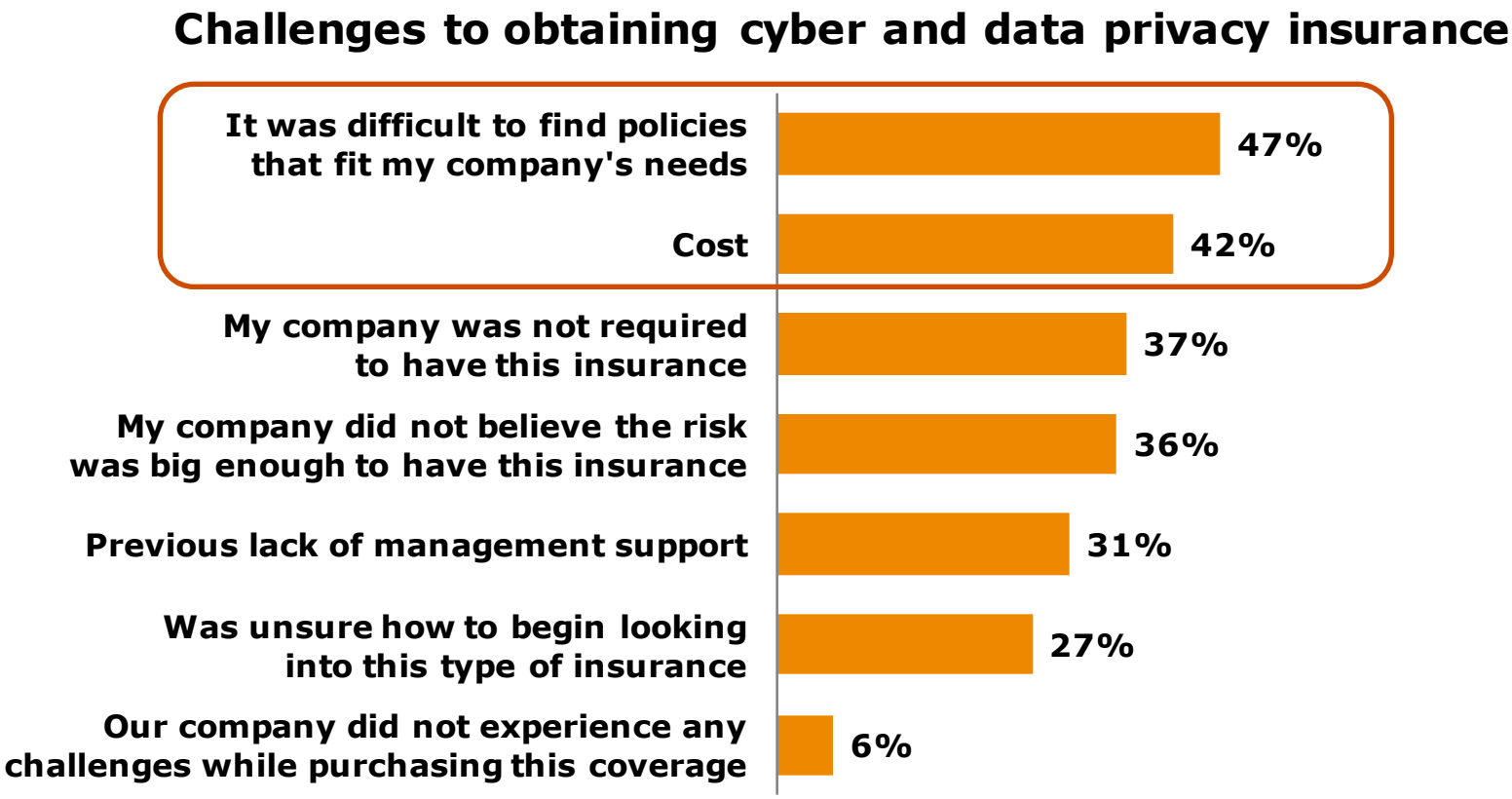


Base: Purchases cyber and data privacy insurance (n=84)

- Q.A4: Which of the following describes why your company purchased cyber and data privacy risk insurance?
- Q.A4_1: What was the *most important* reason why your company purchased cyber and data privacy risk insurance?

Notes:
Numbers shown in **green** in callout bubbles denote statistically higher proportions at 95% level

2015 Wells Fargo Insurance study



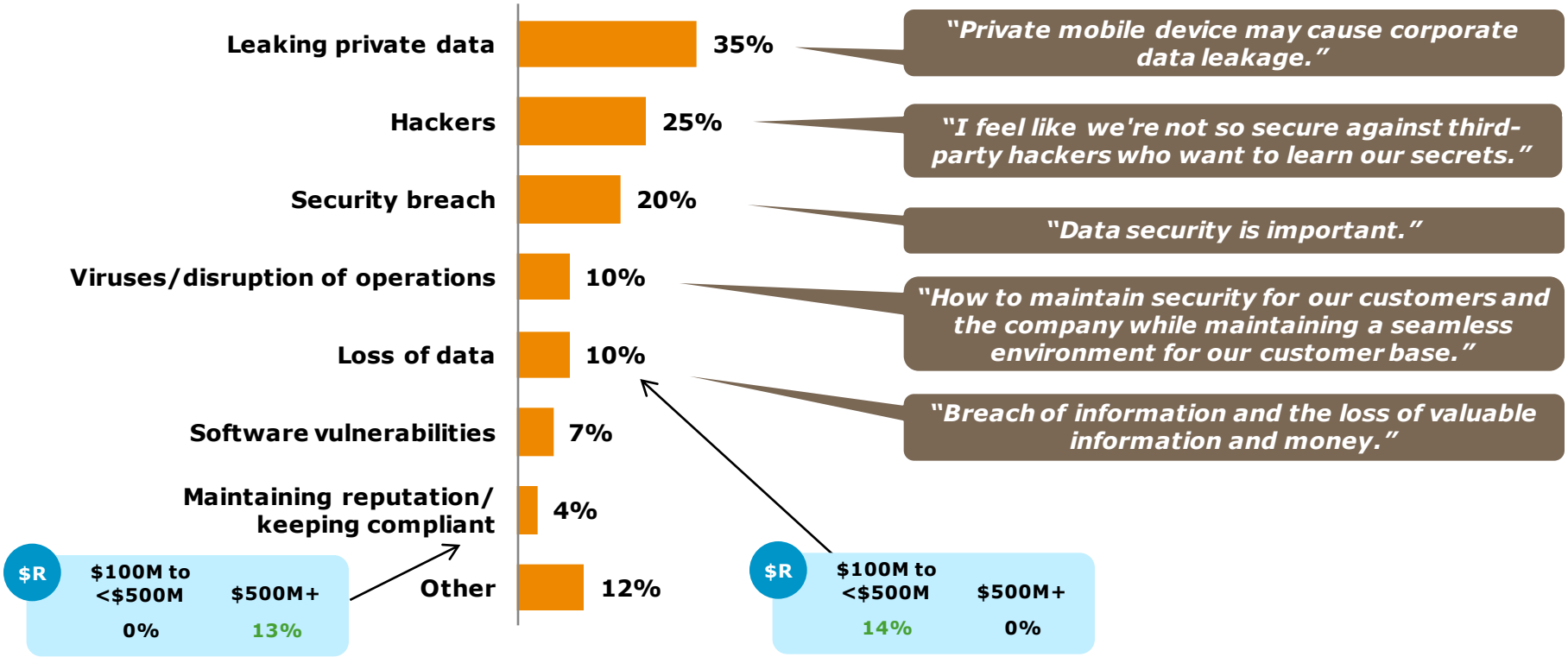
Base: Purchases cyber and data privacy insurance (n=84)

- Q.A5: Which of the following, if any, have been challenges to obtaining cyber and data privacy risk insurance? (Select all that apply.)

Managing the risks

2015 Wells Fargo Insurance study

Top cyber and data privacy concerns



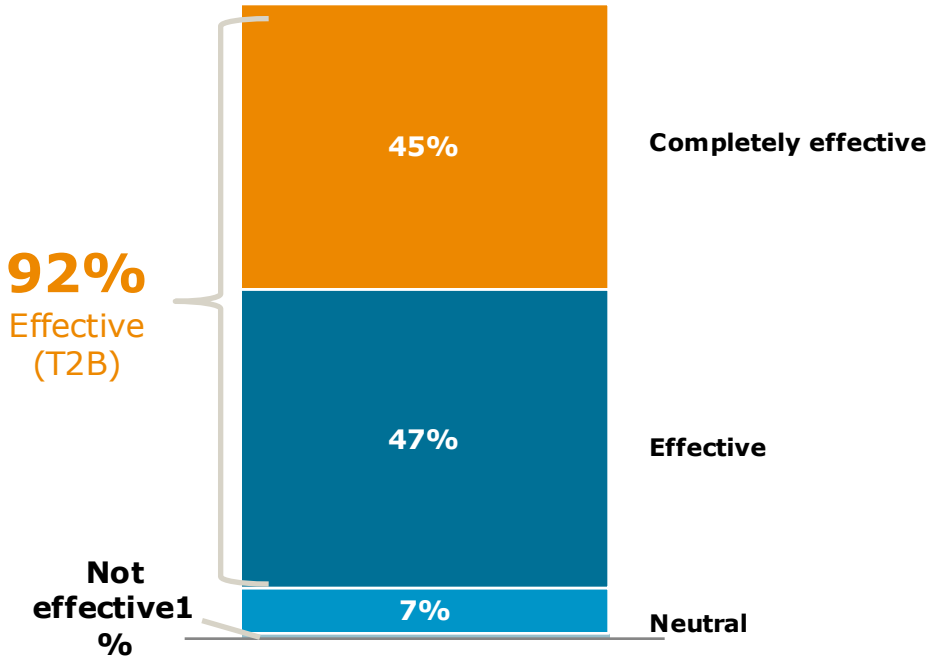
Base: Total (n=72^)

- Q.A1_1: What are your primary cyber and data privacy concerns for your company? (Open end)

Notes:
^"Refused" answers excluded from base
Numbers shown in **green** in callout bubbles denote statistically higher proportions at a 95% confidence level

2015 Wells Fargo Insurance study

Effectiveness of network security intrusion plan



Base: Has had to use network security intrusion plan (n=69)

% of plan revised after most recent use of network security intrusion plan

(Base too small to show percentages)

Percentage	Frequency
0%	2
1-25%	4
26-50%	5
51-75%	10
76-99%	4
100%	2

Base: Has had to use network security intrusion plan (n=27**)

- Q.B4: Thinking about the most recent time you used your plan for a network security intrusion, how effective was the plan?

Notes:

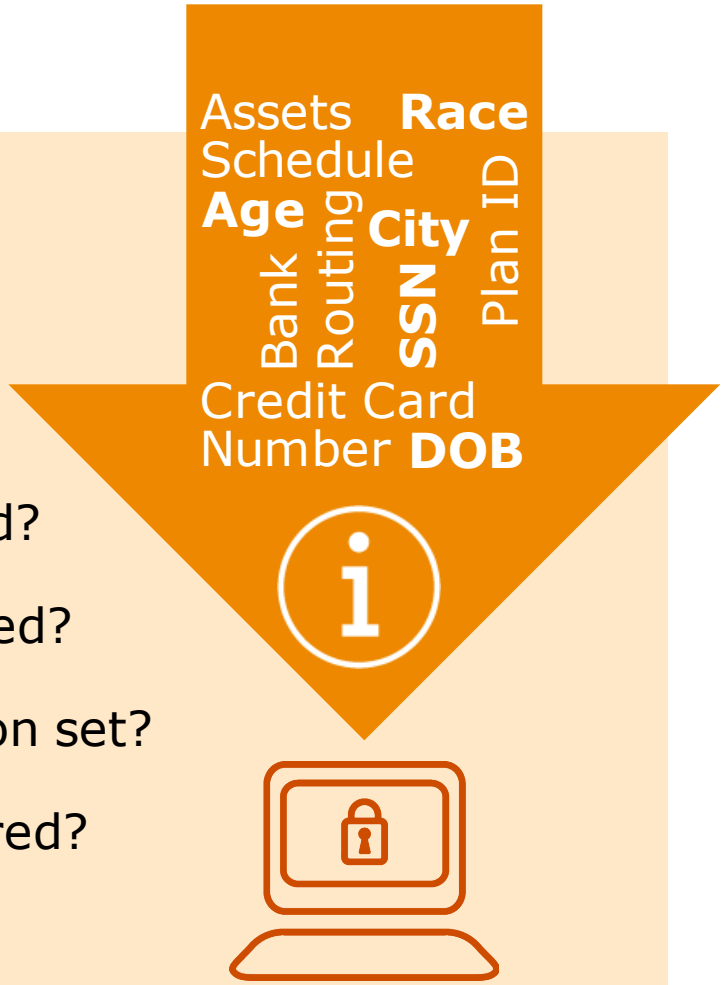
B4 scale: 1=Not at all effective; 5=Completely effective

**B5_N: Results gathered from a re-contact survey among respondents who completed the initial survey; resulting frequencies are not weighted

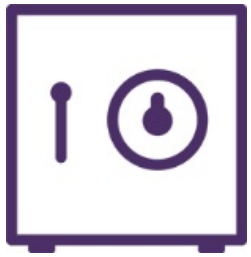
The digital shadow

Can you answer the following questions:

1. What information is being captured?
2. Where is information being captured?
3. What is the value of our information set?
4. With whom is our information shared?
5. How do we protect it?
6. How do we destroy it?



Where is the payroll file?



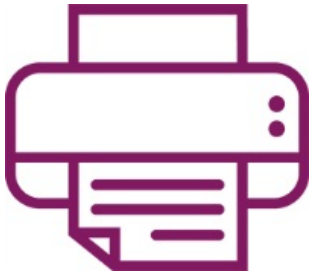
Dropbox

Email

Cloud

Payroll

Laptops



Printer

System servers

Thumb drives, external portable hard drives

Text messaging services

Managing the risks

Response:

- Discovery of data event/ timing
- Incident Response Plan
- Facts
- Law
- Vendors
- Regulatory investigation

Overreact or underreact?

Quick responders spend **54% more** than slow responders.

but…

Response can factor into lawsuits and reputational harm!

Source: Ponemon Institute

Managing the risks

Wells Fargo Insurance

Dena L. Cusick

Tel: (704) 553-6002

Email: dena.cusick@wellsfargo.com

Greg Jones

Tel: (843-573-3560)

Email: greg.a.jones@wellsfargo.com

Thank you