



UNICO

PROTECTING YOUR BUSINESS WITH CYBER LIABILITY COVERAGE

Paul Hughes, CLCS Risk Advisor

Where Connections Make a Difference

unicogroup.com

Three topics addressed today

- ▶ No matter what size of company or what industry they are in, every company is at risk from cyber threats
- ▶ The financial impact of claim
- ▶ Items you want to make sure are incorporated into your cyber risk management program



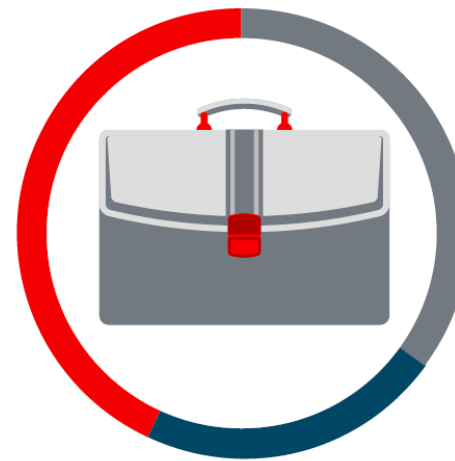
Personal Identifiable Information

- ▶ Name or Address
- ▶ Social security #
- ▶ Driver's license #
- ▶ Bank account #'s
- ▶ Patient/medical info
- ▶ Credit card #'s



Every single entity is in possession of PII

- ▶ If you have employees, you have are at risk.
- ▶ Doesn't matter size of business.
- ▶ 43% of all targeted attacks were on small businesses (chart)
- ▶ Cyber threats are steadily increasing, criminals are becoming more creative each day.



35% ARE LARGE
BUSINESSES

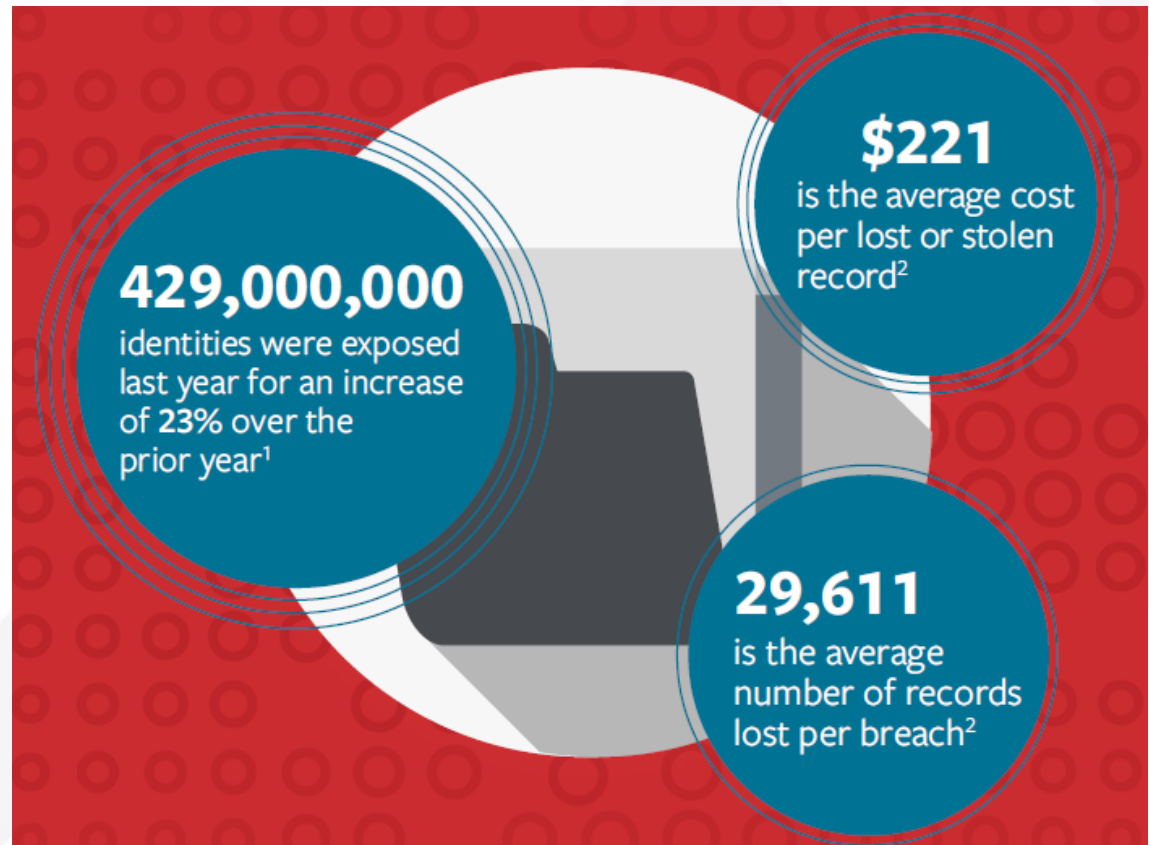
22% ARE MEDIUM
BUSINESSES

43% ARE SMALL
BUSINESSES



In the Event Personal Identifiable Information is Compromised....

- ▶ Businesses are required by law to notify those whose data was compromised.
- ▶ This alone can have a very negative financial impact on a business if cyber liability coverage is not in place



Financial Impact Can be Costly

- ▶ Victim notifications
- ▶ Credit monitoring
- ▶ Forensic IT investigation
- ▶ Retrieval or restoration of data
- ▶ Public relations (loss of reputation)
- ▶ Regulatory concerns / Legal assistance
- ▶ Loss of customers (loss of income)



Costly cont...

- ▶ Not having a cyber policy in place makes an entity four times more likely to face legal action than an entity with cyber coverage in place.
- ▶ Average cost of a cyber breach in 2015 was \$674,000 (According to NetDiligence)



How Insurance Responds

Incident Response

Coach Services

Legal Services

Forensics

Notification

Credit Monitoring

Public Relations

First-Party

Extortion

Interruption

Restoration

Cyber Crime

Third-Party

Network Liability

Media Liability

Privacy/Regulatory
Liability



First Party Incident Response Coverages



Notification

- ▶ Crafting letter or other notification
- ▶ Printing or design
- ▶ Call center operations, mailing or other method of notification
- ▶ Credit monitoring, ID theft prevention, remediation



Public Relations

- ▶ Crisis Management Consulting
- ▶ Public Relations, Advertising & Press Releases



Forensics

- ▶ Costs of forensic examination
- ▶ Costs to remediate discovered vulnerabilities



Legal

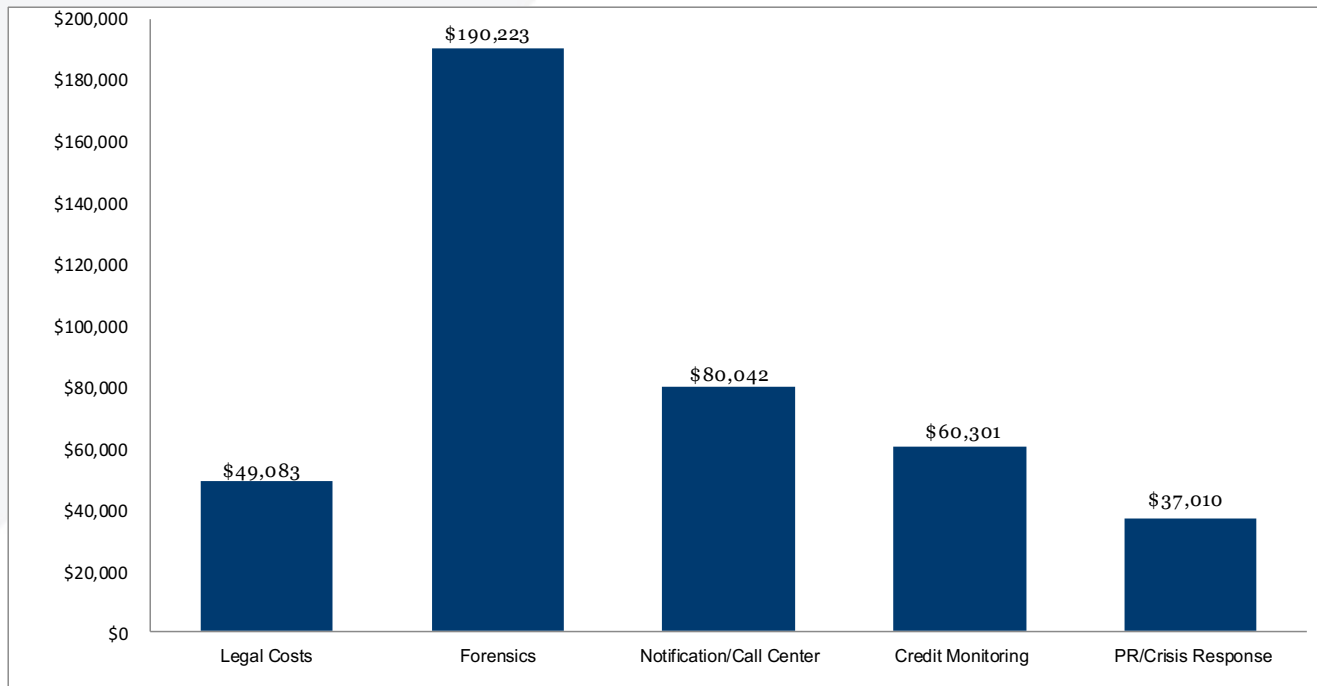
- ▶ Legal representation
- ▶ Regulatory Actions

Additional Extensions

- ▶ Business Interruption, Contingent Business Interruption, and Extra Expenses
- ▶ Network Extortion
- ▶ Digital Asset Loss



Average Costs

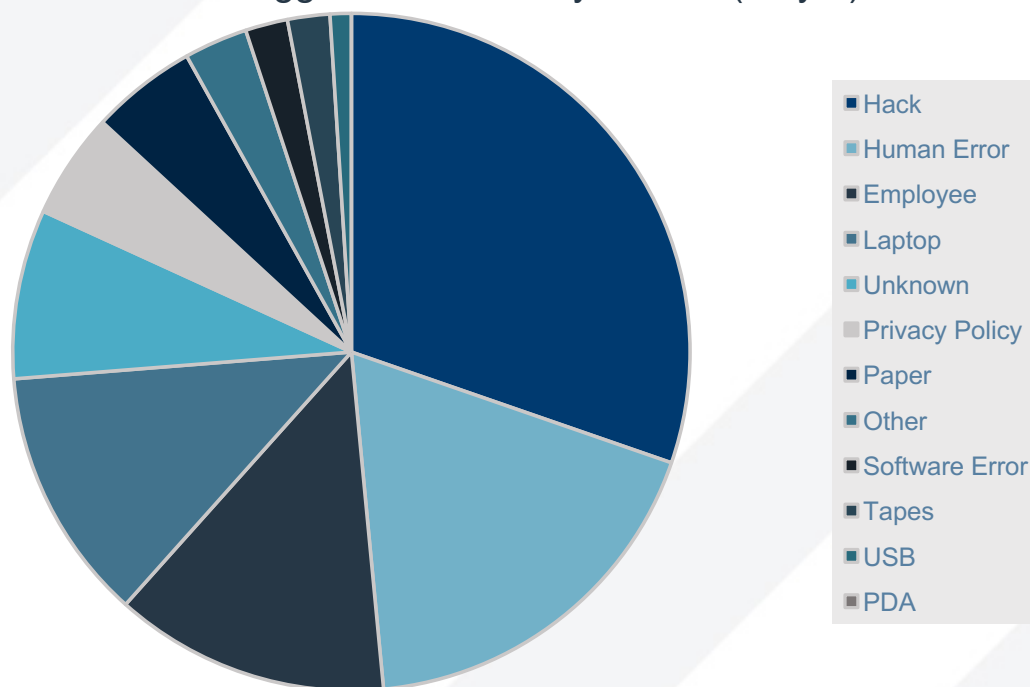


*Based on Chubb claims data as of August 2016



Where do claims actually come from?

Triggers and Industry Trends (10 yrs)



Industry Breakout as of 10/2016

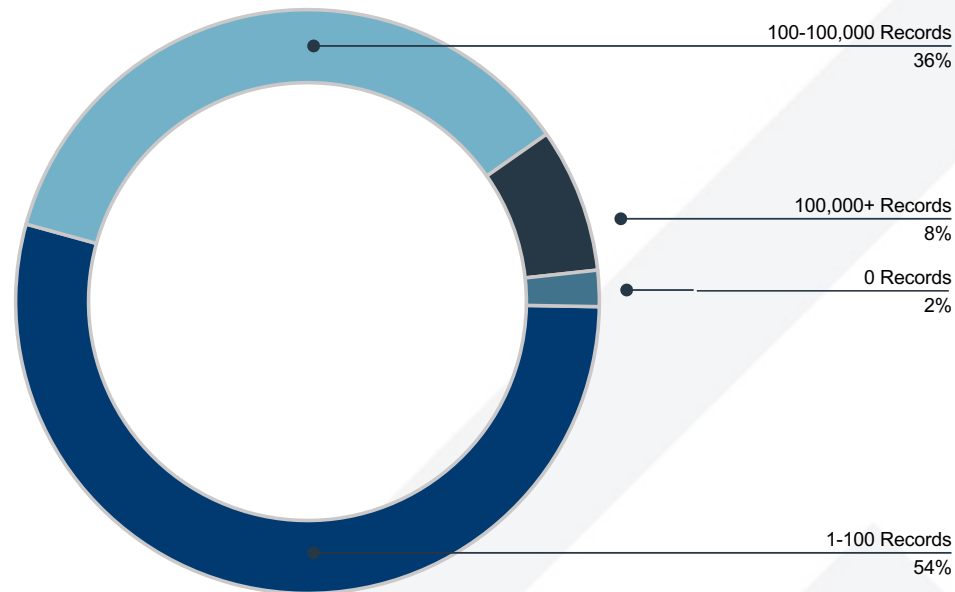
- Healthcare – 31%
- Technology – 9%
- Professional Services – 15%
- Retail – 9%
- Financial Institutions – 6%

*Based on Chubb claims data as of February 2017



Number of Records Compromised

Percentage of Claims Based on Known Number of Records Compromised



Triggers by Industry Segment (as of 10/30/2016)

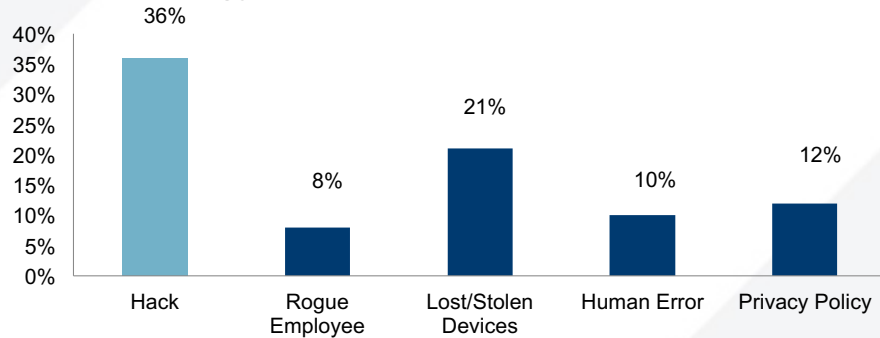
Healthcare



Retail



Technology



Professional Services



Two Parts to a Cyber Policy

- ▶ 3rd Party covers claims arising from failure to notify victims, negligence of managing data, and governmental claims made as a result of the lack of information security.
- ▶ 1st Party coverage addresses the following notification expenses, data restoration, business interruption and public relations.
 - Make sure to include computer fraud and funds transfer fraud
 - According to the Secret Service Cyber Task Force in NE alone there was \$38 million in fraudulent wire transfers in 2014



Analyzing Your Risk Management Platform

- ▶ Cyber threats are becoming more and more creative with social engineering being the newest threat.
 - Social Engineering is not included in almost all cyber policies. You need to request this coverage (sometimes it falls with a crime policy and not the cyber policy)
- ▶ Make sure your cyber policy incorporates a crisis management service so your employees are
- ▶ Not having to follow all of the steps and procedures following a cyber claim
 - By doing this you help eliminate the threat of legal action and maintain the productivity and profitability of your business





| UNICO

THANK YOU!

Where Connections Make a Difference

unicogroup.com