DO SMALL BUSINESSES NEED CYBER INSURANCE?

CYBER SECURITY SUMMIT 2016

PRESENTED BY:
JAKE OMANN, CIC, CPCU

Associated

Associated Financial Group

Why Are you Here?

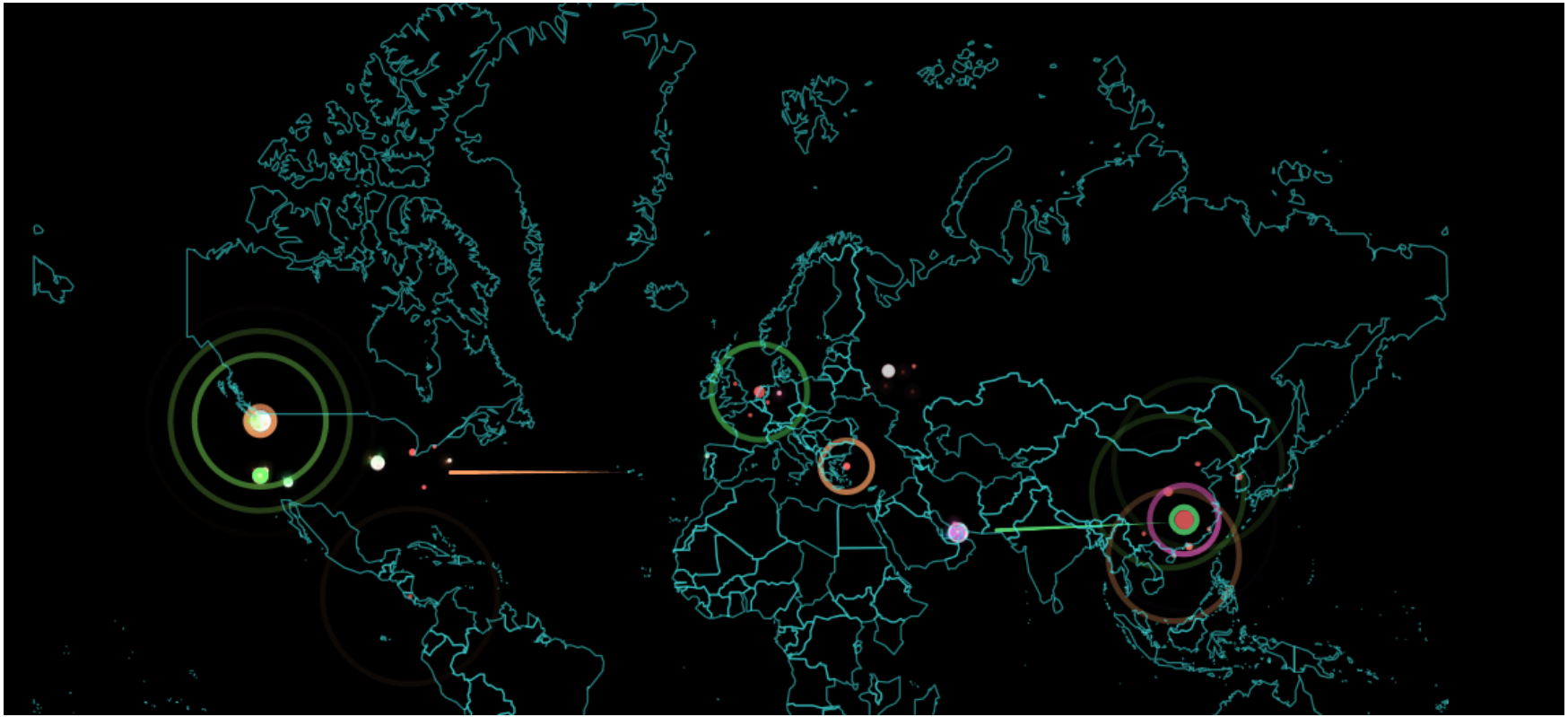
"There are only two types of companies: those that have been hacked, and those that will be."

"Even that is merging into one category: those that have been hacked and will be again." FBI Director Robert Mueller (retired)

AGENDA

- Legal and Threat Landscape
- Cyber Breach Analysis
- Cyber Insurance Overview
- Risk Management Tips
- Q&A

CYBER RISKS AND INDUSTRY TRENDS



CYBER RISKS AND INDUSTRY TRENDS

Public outcry from these risks has resulted in various federal (and state) laws

Health Insurance Portability Accountability Act (HIPAA) (HITECH breach notification rules)

Fair & Accurate Credit Transactions Act (Red Flag Rules) under FTC

State Breach Notification Rules

Gramm Leach-Bliley Rules

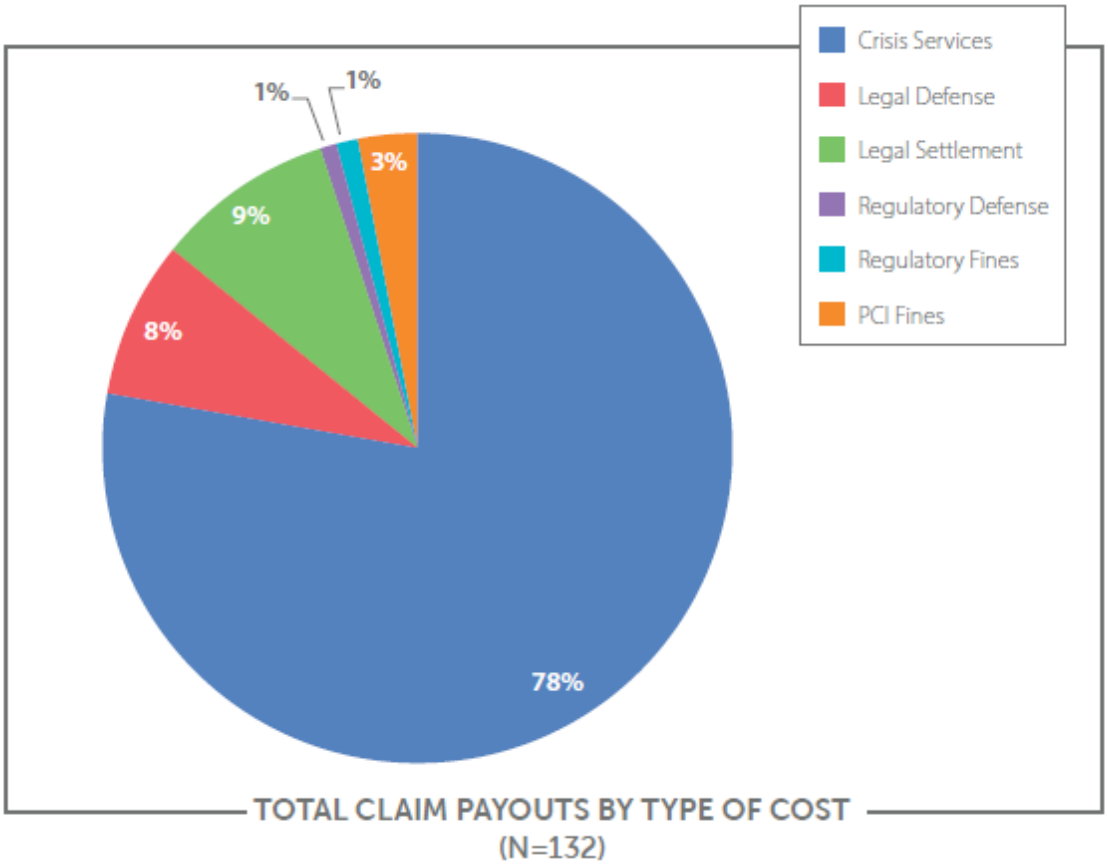
Federal Breach Laws…….

CYBER RISKS AND INDUSTRY TRENDS

Information maintained in data systems often represents highly confidential and “sensitive” information:

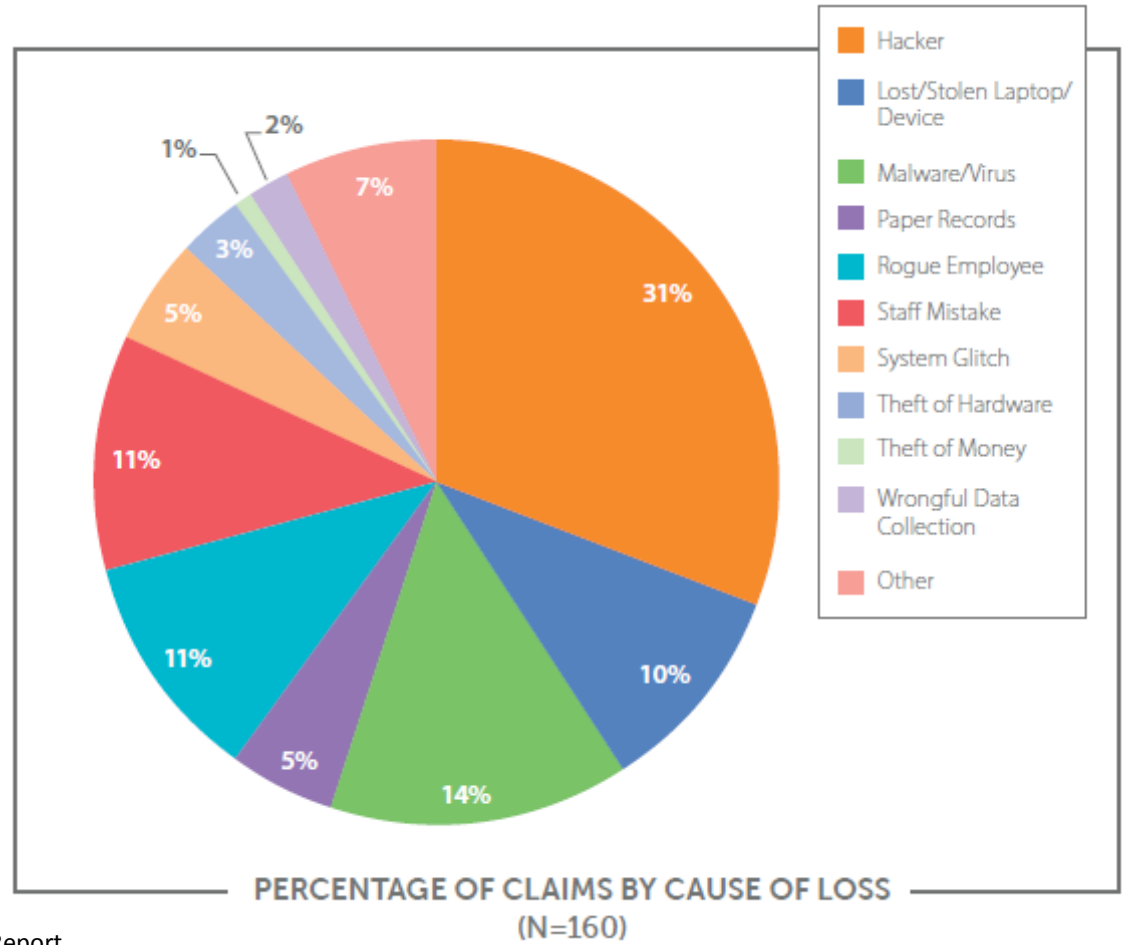
- Financial
- Medical
- Social Security Numbers (DOB, maiden name)
- Credit information
- Immigration documentation
- Intellectual property (patents, trademarks and copyrights)
- Customer proprietary information

BREACH COSTS BREAKDOWN



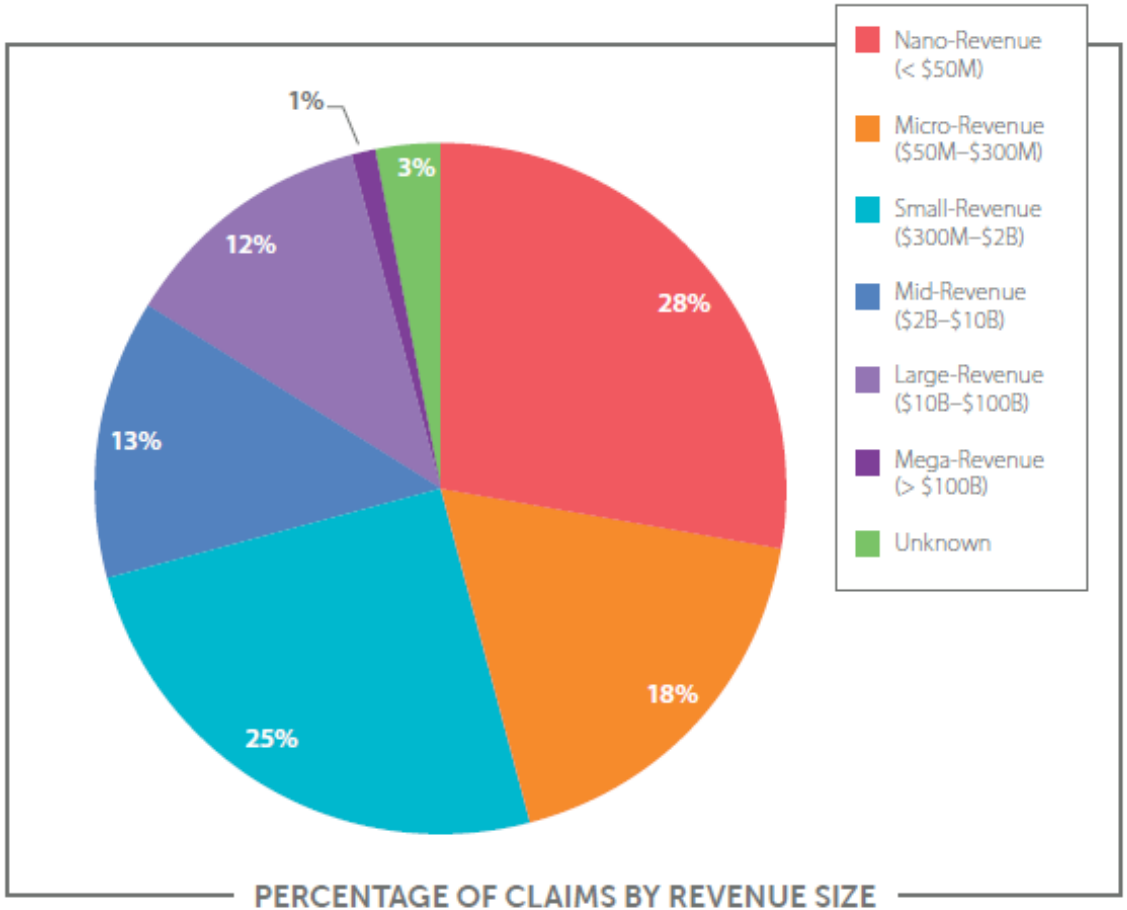
Source: Netdiligence 2015 Cyber Report

BREACH SOURCES



Source: Netdiligence 2015 Cyber Report

COMPANY SIZE BREAKDOWN



Source: Netdiligence 2015 Cyber Report

CYBER LIABILITY COVERAGE – 1ST PARTY

Business income/dependent business income loss	•Reimbursement of loss of income due to a suspension of computer systems (time frame deductible). Reimbursing loss of income due to a data breach to a dependent business partner during the policy period.
Notification and credit monitoring/crisis management	•The cost of notifying the individuals whose data has been compromised and the offering of services to monitor suspicious credit activity.
Data asset restoration/ forensics/ legal/compliance	•Reimbursement of costs to recover, reinstate and recreate intangible assets destroyed during a cyber attack. Forensics obtained to determine what and whose information was stolen. Legal/compliance to determine regulatory and statutory requirements.
Cyber extortion threat	•Reimbursing investigation expenses and ransom payments resulting from malicious threats to your organization's computer system.

CYBER LIABILITY COVERAGE – 3RD PARTY

Privacy liability/employee liability	• Class actions and suits brought (including employees) which result in a monetary payment due to the disclosure of a person's private and confidential information.
Regulatory defense and civil penalties	• Investigation, fines and penalties that you are legally required to pay
Media liability	• Legal liability arising from media content transmitted on any computer system. Harm suffered by others due to an infringement of an intellectual property right. Defamation and slander.

STEPS FOR REDUCING CYBER RISKS

Identify the legal and regulatory requirements applicable to your industry

Audit and upgrade your systems, policies and procedures accordingly

- Identify and implement appropriate training and vetting practices for respective personnel

Evaluate current contracts with third parties and perform due diligence

Evaluate your risk management strategy

QUESTIONS?

Associated

Associated Financial Group