Presenters

Mark Greisiger
President, NetDiligence®

Jay Schulman
Principal, RSM US LLP
Great Lakes Security & Privacy Practice Leader
Cyber risk landscape facing nonprofits

NetDiligence®
About NetDiligence®

• 15+ years supporting the cyber liability insurance industry

• For loss control service, we support the majority of cyber liability insurance markets

• We conduct cyber risk assessments on organizations – and their vendors – all sizes and sectors

• We build/host Breach Response Plans

• We also support most (60+) cyber risk insurers – and their insured clients – with post data breach crisis support via eRisk Hub

Sampling of insurers we support:

- Aegis
- AIG
- Allianz
- Arch
- Argo
- Aspen
- Axis
- Barbican
- Beazley
- Berkley
- Berkshire Hathaway
- Brit
- Chubb
- Cuna Mutual
- Endurance
- Hiscox
- HSB
- Ironshore
- Kiln
- Liberty
- Markel
- National League of Cities
- One Beacon
- Philadelphia
- Principia
- QBE
- RLI
- Starr
- Swiss RE
- Travelers
- Trans Re
- USLI
- Vela
- XL
- Zurich
Mark Greisiger

• **Mark Greigiger** leads NetDiligence®, a Cyber Risk Management company.

• For the past 14 years NetDiligence® has been offering unique cyber risk assessment services to organizations in all sectors.

• ND services support the cyber risk management and compliance needs for businesses.

• ND supports the data breach crisis response needs for most commercial insurers that offer cyber liability coverage.

• Mr. Greisiger is also a frequently published contributor for various insurance and risk management publications on similar topics.
Why are we here?

Organization’s Top 5 Concerns

- Cyber security, cyber risk: 56%
- Changing legislation: 53%
- Corporate liability: 37%
- Natural disasters: 36%
- Talent and skills shortage: 33%
WHAT IS CYBER?

WHERE?
- ONLINE
- OFFLINE

WHO?
- MALICIOUS
- ACCIDENTAL
- INTERNAL
- EXTERNAL

WHAT?
- TECHNOLOGY
- MEDIA
- DATA

Source: Toby Merrill, Chubb
Tip of the iceberg! …many more (most) undetected or not reported

Breaches unreported or not discovered

DataLossDB.org Incidents Over Time
Nonprofit worry: Data is everywhere!

Most organizations are:

- Highly dependent on technology
- Collecting/sharing vast private data
- Continuing to outsource (CLOUD)
- Replicating data everywhere
- Finding it difficult to trace data flow (i.e. your data is not in your Cloud’s Cloud)

Data and dependencies are everywhere: (1.) Servers (2.) Corp Databases/Web Applications (3.) Remote Users (Laptops/iPhones) (4.) Back-Up/Storage Facilities (5.) Service Providers/CLOUD (5.b) The Clouds for your Clouds (6.) Contractor systems (7.) Credit Card Processors (8.) Mobile Apps (9) Your ‘Big Data’ analytic marketers, etc.
Cyber threats facing nonprofits

- **Insiders:** Malicious and disgruntled employees
  - Changing data/deleting data/destroying data or programs with logic bombs(crashing systems/holding data hostage/stealing and selling data/entering data incorrectly)

- **Outside attackers** (they don’t know you and don’t care if you’re large or small)
  - Intrusion/hack
  - DDoS
  - Social Engineering (Phish Fight)
  - Email Hacking
  - Extortion

- **Viruses & Malware**

- **Non-Malicious – employees** (email and mailing errors, or lost laptops)

- **Non-Malicious – system/coding glitch**

- **Trusted Third-Party: BA Vendor/Cloud Breach or Mishap** (they control your data or system)
Growing nonprofit concern: Class action liability

Privacy Data Breach Cases
State and Federal Courts

- Felder v. B.C. Davidson (2008)
- Gandolfi v. Aurora Health Care (2009)
- Proctor v. Old Navy (2007)
- Eiker v. Little Janie's (2007)
- Stetevens v. Tri-West Healthcare Alliance (2005)
- Parise v. Wells Fargo (2006)
- Chandiah v. Fifth Third (2006)
- Rhee v. United Life & Health Insurance (2010)
- Catlin v. Foreign, North, Porter & Groody (2000)
- Bennett v. TracFone Wireless (2009)
- Sandy v. Dean (2009)
- Rodger v. PNC (2007)
- Zinsmeister v. Fidelity (2009)
- Rabinowitz v. Discover (2005)
- Walker v. ENL (2005)
- Gartner v. Ernst & Young (2010)
- Itami v. VideoBank Communications (2007)
- Keller v. Mason County Greyhound Park (2011)

- Credit Card Processing v. USA v. Manafort Bank (2011)
- Tr Media v. AMAG (2008)
- Valley v. Gas Communications (2011)
- Frazier v. Mobile (2009)
- Pennsylvania State Employees Credit Union v. Fifth Third Bank & B.N. Wholesale Club (2008)
- Oracle v. Deckard One Services (2010)
- Wexford v. Preferred Health System (2005)
- Office v. PNC (2003)
- Madsen v. PNC (2003)
- Atwood v. Union Bank (2007)
- Bank of America Foundation (2006)
- Rabinowitz v. Mid-Maine (2007)
- Griffin v. First Marng Bar (2008)
- Clark Street Real Estate v. Empresas (2002)
- Perry v. Atlantic Health Insurance (2007)
- Brown v. PNC (2007)
- McIntyre v. Jewish Hospital & St. Mary’s Healthcare (2010)
- Lepowsky v. Converse (2009)
- Website v. Equifax (2010)
- Law v. LinkedIn (2012)
- Villar v. MySpace (2011)
- Kopp v. Chase (2009)
- In re Google User Privacy Litigation (2013)
- Conley v. Taleo (2007)
- Brimmer v. Genesis and Dot-10 (2006)
-ことごと v. Equifax (2009)
- King v. KP (2006)
- Todd v. Target (2010)
- Friedman v. CVS (2010)
- Wiles v. Southeast Bell Telephone (2011)
- King v. Dexplore (2001)
- Clark v. Lessor (2011)
- Godinot v. Equifax (2011)
- Merica v. First Third Bank (2007)
- Rakhmetov v. AZ (2009)
- Noll v. Equifax (2009)
- Cherney v. Wachovia (2008)
Very common technical weak spots (not going away)

- Problem 1) IDS or ‘Intrusion Detection Software’ (bad guy alert system)
  - Studies show that 70% of actual breach events are not detected by the victim-company, but by third parties (and many more go undetected completely)
  - FTC and plaintiff lawyers will cite ‘failure to detect’
- Problem 2) Encryption (of private data every node)
  - Very rarely used P2P or across a full enterprise (email, web app databases, laptops, clouds, etc.)
- Problem 3) Patch Management - Challenges:
  - All systems need constant care (patching) to keep bad guys out
  - Verizon DBIR 2016: Over 85% of breaches caused by old/known exploits (Top 10 CVEs. Over 1 year to 7 years old)
- Problem 4) Vendor Mis-Management
  - Vendors more often now in care, custody and control of your systems or data
  - Often no oversight; little due diligence
  - SLAs often disown security assurances (no defense or indemnity contractual provisions; waive right to subrogation)
  - 1 of 3 events caused by third-party vendor
**Sample Size** = 176 claims

**Per Breach Costs**
- **Average breach cost**: $665K
  - *Comment: more representative of ‘main street’ than Wall Street*
  - *Small organizations = 87% of claims.*
- Large organizations: $6M (up from last year)
- Healthcare: $717K

**Per Record Costs**
- **Average per-record cost**: $17K* (median cost = $40)
  - *Spiked average due to 3 big ‘outlier’ claims; one was over $1M per record!*
- **Cost Range**: $0.03-$1.6M (pennies to millions)
• Crisis Services Costs (forensics, legal counsel, notification and credit monitoring)
  - **Average cost:** $357K (median: $43K)
  - *Breach Coach®* lawyers helping control crisis costs

• Legal Costs (defense and settlement)
  - **Average cost of defense:** $130K (median: $16K)
  - **Average cost of settlement:** $815K (median: $250K)
NetDiligence® 2016 Cyber Claims Study

HIGHLIGHTS OF FINDINGS

COMPARING 2016 TO PRIOR YEARS

Average number of records exposed and cost by type (in millions)

- # of Records
  - 2014: 2.4
  - 2015: 0.8
  - 2016: 3.7

- Per-Breach Cost
  - 2014: 1
  - 2015: 0.7
  - 2016: 0.4

- Crisis Services
  - 2014: 0.4
  - 2015: 0.5
  - 2016: 0.7

- Legal Defense
  - 2014: 0.7
  - 2015: 0.4
  - 2016: 0.1

- Legal Settlement
  - 2014: 0.6
  - 2015: 1.2
  - 2016: 0.8
NetDiligence® Claims Study
HIGHLIGHTS OF PRELIMINARY FINDINGS

Data Type

- PCI: 28%
- PHI: 15%
- PII: 40%
- Non-card Financial: 5%
- Other: 7%
- Unknown: 2%
- N/A: 5%

Cause of Loss

- Hacker: 22%
- Lost/Stolen Device: 12%
- Malware/Virus: 20%
- Paper Records: 9%
- Rogue Employee: 7%
- Staff Mistake: 7%
- System Glitch: 14%
- Theft of Hardware: 6%
- Theft of Money: 1%
- Wrongful Data Collection: 1%
- Other: 1%
- Unknown: 1%
- System Glitch: 2%
- PCI: 2%
Cause of loss for nonprofits (a deeper look)

Cause of Loss Chart

**INTRODUCTION**
Explore the causes of loss for a given industry.

**Select Industry:**
- Education

**Health Care**
- Environmental - 0.33% (5)
- Error - 20.34% (536)
- Hacking - 8.51% (120)
- Malware - 2.00% (31)
- Mitigae - 22.51% (341)
- Physical - 59.07% (801)
- Social - 0.09% (9)

**Education**

**Health Care**

Health Care (1515)

Physical (26)

©2017 RSM US LLP, All Rights Reserved.
NetDiligence® Claims Study

HIGHLIGHTS OF FINDINGS

**Business Sector**
- Entertainment: 2%
- Financial Services: 10%
- Gaming & Casino: 1%
- Healthcare: 19%
- Hospitality: 6%
- Media: 2%
- Non-Profit: 1%
- Other: 11%
- Professional Services: 20%
- Restaurant: 1%
- Retail: 9%
- Technology: 1%
- Telecommunications: 2%

**Organization Size**
- Nano (<$50M): 87%
- Micro ($50M-$300M): 13%
- Small ($300M-$2B): 6%
- Mid ($2B-$10B): 5%
- Large ($10B-$100B): 1%
- Mega (> $100B): 2%
- Unknown: 27%
Example cyber claims/loss

1) Healthcare organization
   • Profile:
     • $100M revenue
     • Lost only 130 records (PHI breach)
   • Loss: **$301K**
     • $51K defense
     • $250K HIPAA/AG fines

2) Healthcare organization
   • Profile
     • $50M revenue
     • Lost 10,000 records (PHI breach)
   • Loss: **$256K**
     • Victim notice: $45K
     • Credit Monitor: 0
     • Legal/Breach Coach: $101K
     • Forensics: $110K
What can nonprofits do? Assess your readiness

Purpose: Showcase Strengths & ID Weakspots
• Build on PCI/ HIPAA etc
• Focus: Privacy & Security Liability
• Reaffirm ‘reasonable’ safeguards
• Benchmark to Standards & Peers
• Show good faith effort to compliance with Regs
• Doc your Cloud Usage/Partners
• Show lessons learned from past incidents (battle ready stance)

Cyber Risk Insurability Assessment
• Process should be collaborative
• Educate CEO about their own IT operations
• Wide-Angle: people, process & tech
Preparedness tips for nonprofits

• Perform a **Cyber Risk Assessment**
  - Include any third-party IT & data storage dependencies (contractors, clouds, etc.)
  - Map your sensitive client data
  - Review privacy with security (e.g. wrongful data collection exposure)

• Develop and operationalize a **data breach Incident Response Plan**
  - Bolster your IRP... Self-help with outside experts
  - Tiger Team experts
    - Breach Coach® (legal expert)
    - Computer Forensics (triage and establish the facts who, what, when, where and how)
    - Notification and call center
    - Credit & ID Monitoring
    - Public relations

• Conduct training on a regular basis to all employees and vendors
• Review insurance coverage for gaps, ensure ‘cyber liability’ (not just E&O)
Thank you!

Mark Greisiger
NetDiligence®
Mark.Greisiger@NetDiligence.com
610.525.6383
CYBERSECURITY

The latest statistics
Security statistics

Compiled from:
- NetDiligence® 2016 Cyber Claims Study

PERCENTAGE OF RECORDS EXPOSED BY DATA TYPE
(N = 120)
30% of breaches were due to insiders. Of those, 77% were unintentional.
Security statistics (continued)

Compiled from:
- NetDiligence® 2016 Cyber Claims Study

**PCI FINES**

5% of claims included costs for PCI fines. Payouts for PCI fines ranged from $3,000 to $3M.

<table>
<thead>
<tr>
<th>Claims with Costs</th>
<th>Total</th>
<th>Min</th>
<th>Median</th>
<th>Mean</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCI</td>
<td>8</td>
<td>3,963,285</td>
<td>3,000</td>
<td>58,006</td>
<td>461,661</td>
</tr>
</tbody>
</table>
CYBERSECURITY

Threat overview
Threat modeling methodology

- Threats (How)
- Assets (What/Where)
- Actors (Who)
- Risk Tolerance (Why)
- Mitigations and Assessment Strategy
- Why

Threat Model
Who are the bad actors you’re concerned with?

- Employee
- Contractor
- Customer
- Random attacker
- Focused attacker
- State-sponsored attacker
Threats (How)

How are the bad actors going to attack you?

- From the Internet
- From your internal network
- From your wireless network
- Via email
- From USB keys
- From the phone
Assets (What/Where)

What data do they want?
• Customer records
• Employee records
• Money transfer
• Money laundering
• Ransomware

What data elements are they trying to steal?
• Social Security numbers
• Credit card
• W2
• ACH/account number
Every “scenario” has a cost. What is your risk tolerance?

- Financial risk
- Brand risk
- Operational risk
The result is a set of scenarios that are most important to you.

You can use these scenarios to:
• Assess the likeliness of being impacted from them
• Build a strategy to protect yourself against them
• Hedge your losses against them with cyberinsurance
• Accept the risk
Your threats

• Accept the risk
• Build a strategy and continue to assess
• Hedge with cyber insurance
• Rinse and repeat
For more information

Contact us:
• Mark Greisiger - mark.greisiger@netdiligence.com
• Jay Schulman - jay.schulman@rsmus.com

Additional resources:
• Download the NetDiligence® 2016 Cyber Claims Study
• Subscribe to Muse, a bimonthly newsletter dedicated to providing ideas and education to tax-exempt organizations.
Before we conclude

• Register for RSM’s next event:

*Nonprofit webcast series: Benefits of an effective outsourcing strategy*

- **Date:** Wednesday, March 1, 2017
- **Time:** Noon EDT | 11 a.m. CDT
- **Duration:** 60 minutes
- **CPE credit:** Up to 1.0 CPE credits will be issued
- **Register:** rsmus.com/events