ADVISEN
Insurance Intelligence

The Time for Cyber Coverage is Now

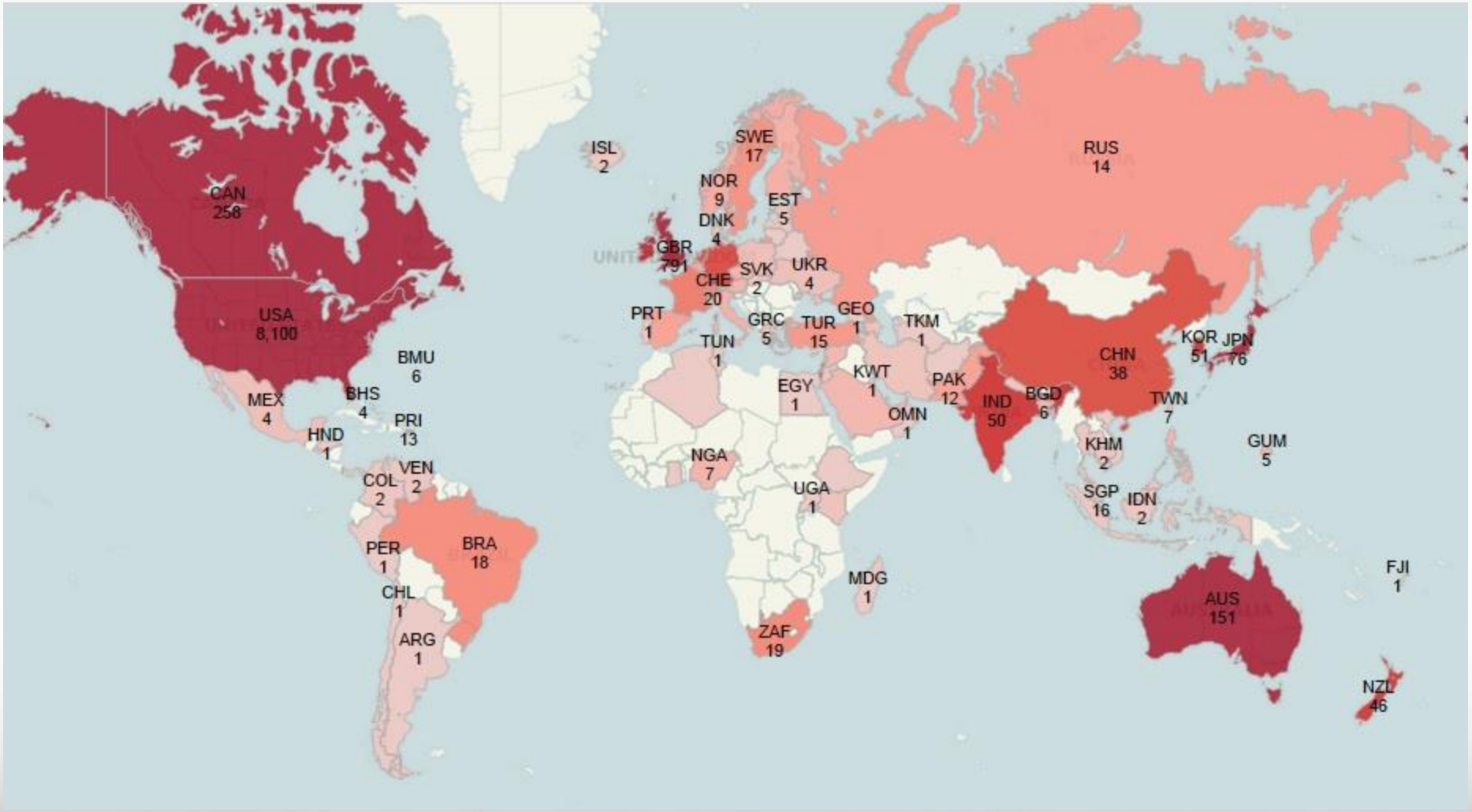
May 14, 2014

TARGET MARKETS
Program Administrators Association
"Where Program Business Gets Done"

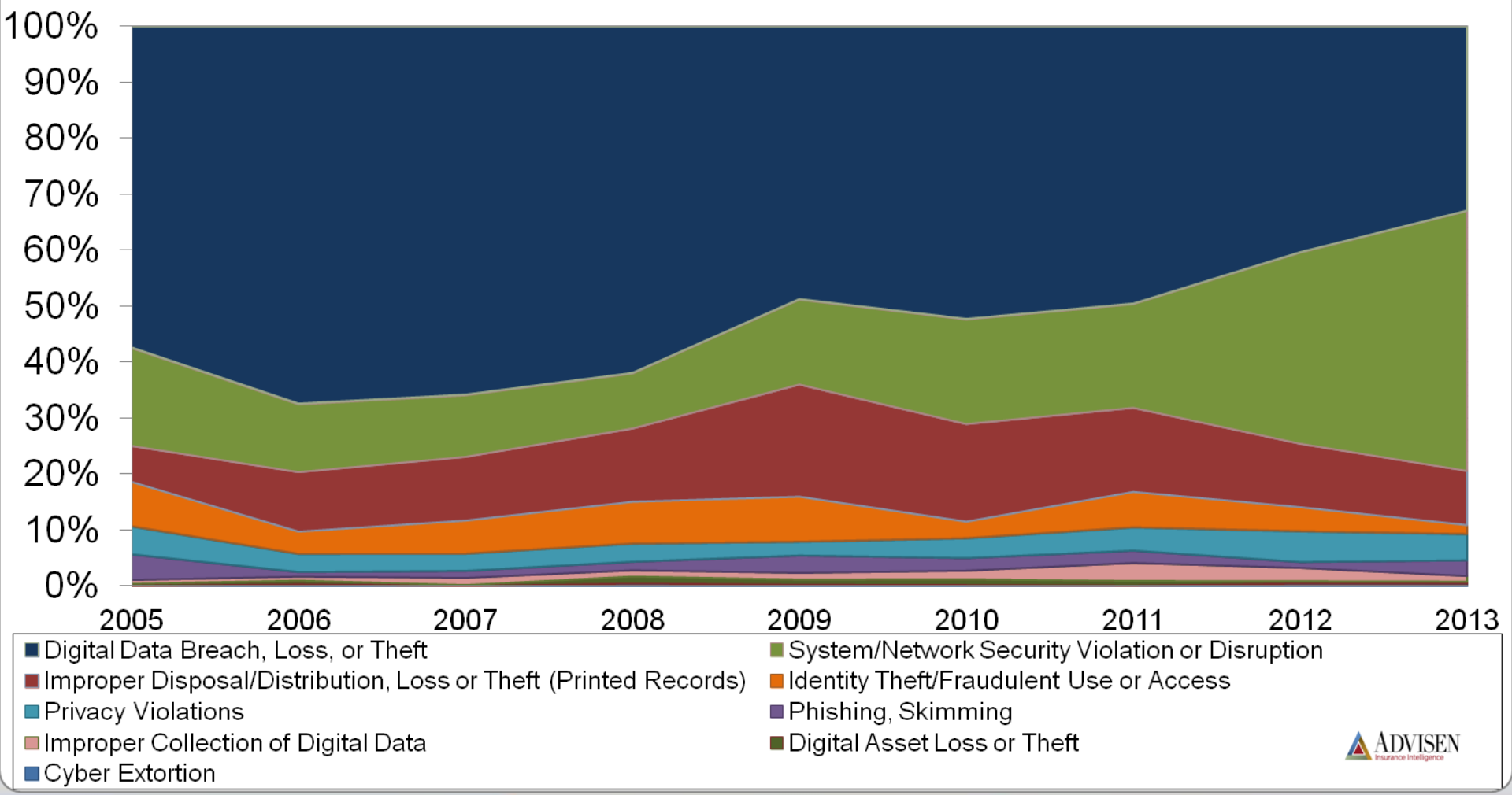
Panelists

Melissa K. Ventrone	Partner and Chair, Data Privacy & Security Group	Wilson Elser Moskowitz Edelman & Dicker LLP
Kevin Ribble	Executive Vice President	Edgewater Holdings
Jim Blinn	Executive Vice President	Advisen Ltd.

Global Cyber Event Heat Map



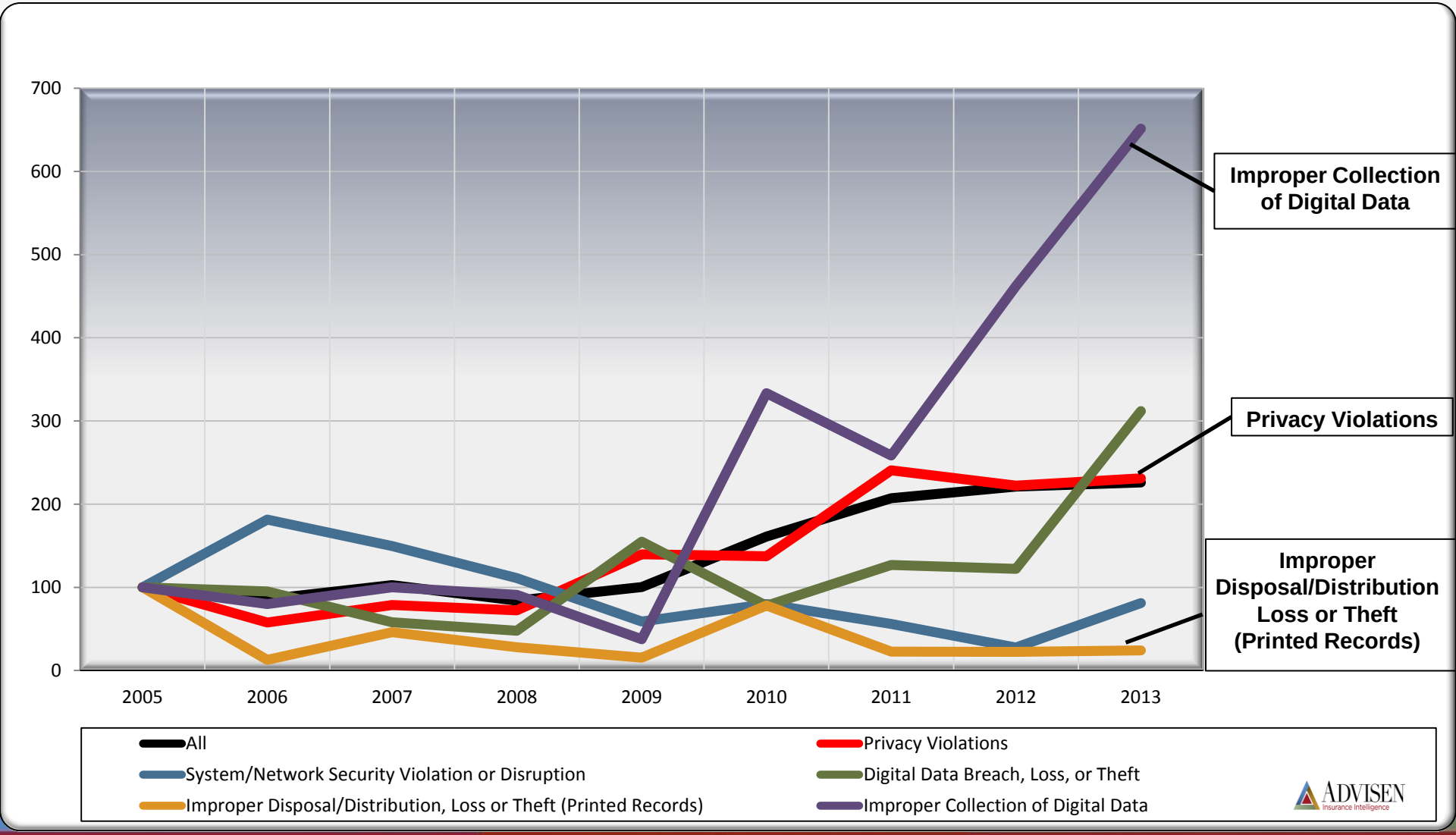
Cyber Event Type Composition by Year



Cyber Events by Company Size

Number of Employees	Event Count	Percentage
0 - 25	1,626	15.9%
25 - 50	571	5.6%
50 - 100	570	5.6%
100 - 250	761	7.5%
250 - 500	515	5.0%
500 - 1,000	544	5.3%
1,000 - 5,000	1,427	13.9%
5,000 - 10,000	638	6.2%
10,000+	3,595	35.1%
Total	**10,247**	**100.0%**

Cyber Litigation Frequency Index



Scenario I: Notification Expense

A large Program Administrator discovered that discovered that around October 2, 2013 unauthorized software was uploaded to their computer system. The investigation revealed that a hacker, through the malicious software, had viewed files containing a username and password. The Administrator immediately disabled the compromised username and password and launched an internal investigation to determine whether the credentials could be used to access personal information stored on system. Unfortunately, the hacker accessed Client names, mailing addresses and other Client data that were stored on the system.

Notification Expenses:

- **Tangible expenses:**
  - Forensic Investigation
  - Public Relations
  - Call center services, notification costs, credit monitoring/identity restoration
  - Lost employee time responding to breach
  - Legal Fees
- **Intangible costs**
  - Loss of customers/clients
  - Loss of business
  - Harm to reputation of business

Policy Questions

- **Crisis Management**
  - Policy apply to attorney fees to draft response to breach and related deliver costs?
  - Is credit monitoring/identity restoration included for individuals?
  - Will policy provide options for notification methods?
- **First Party business interruption**
  - Do they offer contingent period after system restored?
  - Based on time system is down or a stated time period?
  - Wild viruses included

Risk Mitigation

- Defense in depth
  - Technology / Infrastructure
  - Personnel
  - Insurance

Scenario II: Regulatory Investigation

Investigators with the Texas Office of the Attorney General looked into an insurance data provider that does business in Texas, after a Corpus Christi reporter found some of the company's records in an unsecured Dumpster. Documents found in the investigation included customers' personal information, such as names, driver's license numbers and dates of birth. The State of Texas sued the data provider, alleging the company did not have appropriate or secure security measures regarding the private personal information of its customers. The company denied the allegations but settled for $125,000 and agreed to implement an employee security training program.

Regulatory Expenses

- **Compliance with Global Security/Privacy Regulations**
  - Most Triggered by Breached Individual's Residence, NOT Location of Breached Business
- **Impact of Breach on Reputation**
  - Breach is a "Tipping Point"
- **Financial Difficulties Caused by a Breach**

Policy Questions

- **Regulatory Investigations**
  - Which regulatory investigations are covered?
- **Regulatory Proceedings**
  - Which regulatory proceedings are covered?
  - Fines and penalties covered?

Risk Management Strategies

- Education and training
- Auditing and Compliance
- Testing your policies now

System Security Breach – Cyber Theft

On September 20, 2013, Benefits Administrator #1 (Plaintiff) filed a lawsuit against Benefits Administrator #2 (Defendant). The lawsuit was brought in relation to Defendant's alleged breach of Plaintiff's private Oracle database hosted by a cloud service provider. Plaintiff spent over $300,000 and five years to compile the database. On October 2012, Defendant improperly requested and was inadvertently given access by the cloud provider to Plaintiff's database in violation of privacy laws. The database included confidential and private personal information relating to 6,500 NEFNJ contacts. Defendant allegedly took wrongful possession of files relating to NENFJ's finances, including financial records, and personal client files.

Risk Management - Do you know where your information is and who has access?

- **Third Party Vendors** –
  - who has it, why do they have access, and how do they protect it?
  - Vendors of your vendors
- **Cloud Hosting**
- **Data retention/destruction policies**
  - what do you do with the data when you are done with it?

Policy Questions

- **Third-Party Liability**
  - Coverage for transmission of virus to third party and 3rd party to others
  - Copyright infringement from website
  - Full prior acts vs. retro-date inception
  - Coverage applies to both electronic and physical data breaches e.g. paper, laptop, disks, PDA etc. ?
  - Coverage applies to both personal and company information?
  - Coverage applies to employee and customer information – yes
  - Information in care custody or control of insured's vendors include cloud servers and records being transported?
  - Policy apply to accidental losses and leaks?
  - No insider exclusion?
  - Direct intentional attacks are covered is "wild viruses" those not specifically targeting insured?

Summary

- Small Businesses are considered to be at High Risk
- Best Practices can aid in preventing an attack *before* it happens and reducing it after it occurs
- Typical insurance does *not* provide adequate coverage
- Cyber Liability coverage can help bridge the gap