Session 4A: Operationalizing Third Party Risk Management

Moderator:
Randi Woods Webber, FSA, CERA, MAAA

Presenters:
Dana N. Hunt, FSA, MAAA
Charlie Miller
Randi Woods Webber, FSA, CERA, MAAA

ERM Enterprise Risk Management Symposium

Your Meeting, Your Experience.

CAS Canadian Institute of Actuaries Institut canadien des actuaires SOCIETY OF ACTUARIES

ERM Enterprise Risk Management Symposium

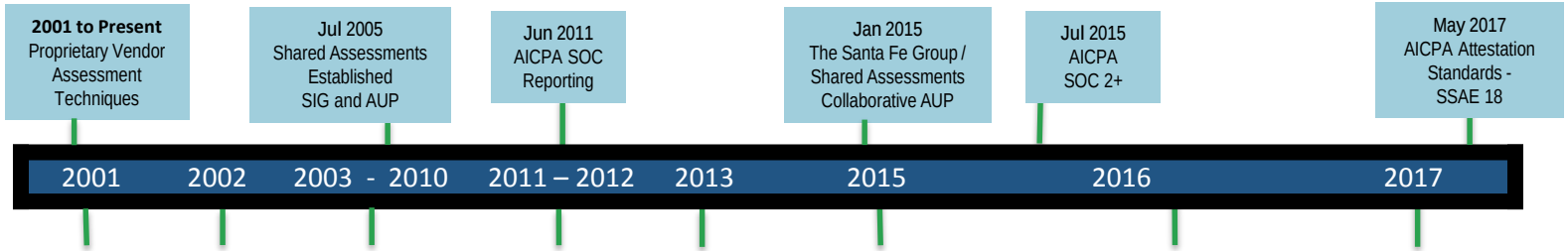
Session 4A:

Operationalizing Third Party Risk

Panelists

- **Randi Woods, VP Operational Risk and Corporate Service Center CRO**
- **Dana Hunt, Director, US Insurance Assurance, PWC**
- **Charlie Miller, SVP, The Santa Fe Group/Shared Assessments Program**

US - Regulatory Landscape - Third Party Risk



Aug 1996
Health Insurance Portability and Accountability Act (HIPAA)

Jul 2001
Graham-Leach Bliley Act (GLBA)

Nov 2001
OCC - Third Party Relationships

May 2002
OCC - Foreign Third Party Service Providers

2003 – 2010
Privacy Breach Notification Laws – Various States

Jun 2008
FDIC - Guidance for Managing Third Party Risk

Jan 2011
Payment Card Industry – Data Security Standards

Jan 2012
FDIC - Payment Processor Relationships Revised Guidance

Oct 2013
OCC - Third Party Relationships: Risk Management Guidance

Dec 2013
FRB - Guidance on Managing Outsourcing Risk

Feb 2015
Technology Exam Handbook: New Appendix for Business Continuity Planning Booklet

Feb 2015
SEC - Report on Cyber Security

May 2015
Payment Card Industry – Data Security Standards V3.0

Jun 2015
FDIC / NIST - Cybersecurity Assessment Tool

Nov 2015
FDIC - Handbook: Revised Management Booklet

Jun 2016
OCC - Cybersecurity of Interbank Messaging and Wholesale Payment Networks

Jun 2016
FDIC - Information Technology Risk Examination (InTREx) Program

Sep 2016
FDIC - Revised Information Security Booklet

Feb 2017
OCC - Third Party Relationships: Supplemental Examination Procedures

Mar 2017
NYS - Cybersecurity Requirements for Financial Services Companies

The Office of the Comptroller of the Currency (OCC) *defines a third-party relationship as any business arrangement between a bank and another entity, by contract or otherwise and it expects a bank to practice effective risk management regardless of whether the bank performs the activity internally or through a third party.*

ERM Enterprise Risk Management Symposium

Headlines Involving Third Parties

HealthIT Security
May 2016

Vendor Data Breach Exposes Info on 87K Patients
A hack of a healthcare provider's software management vendor compromised the personal information of around 87,314 patients, including names, phone numbers, insurance information, and Social Security numbers. Hackers could have accessed the information as early as January 2015, but were not noticed until near the end of March 2016.

Wall St. Journal
January 2014

Target Now Says 70 Million People Hit in Data Breach

Target Corp.'s holiday data breach was bigger than the company had previously said, **penetrating additional systems and compromising a new set of personal information** affecting up to 70 million people.

Target CEO resigns

U.S. Dept. of Health & Human Services
March 2016

$1.55 million settlement underscores the importance of executing HIPAA business associate agreements
An investigation indicated that a hospital **failed to have in place an appropriate business associate agreement**, as required under the HIPAA Privacy and Security Rules, so that its business associate(vendor) could perform certain payment and healthcare operations activities on its behalf.

Info Security Magazine
March 2017

Third Party Hack Exposes Staff Details
Thousands of staff had their details exposed after a data breach at a private contractor. Hackers gained access to IT systems belonging to a company who handles data on behalf of the healthcare company.

Digital Guardian
October 2016

Third Party Data breach problem
A hack of a digital media vendor led to compromises of online photo services at several large retailers as well as a healthcare company and a targeted group of its clients.

Financial Express
March 2017

A social media service was hacked through an app hosted by a third party, triggering a torrent of swastika-filled posts for several high-profile accounts.

ABA 2016 Tech Report

A survey revealed that 26% of the largest legal firms (500 or more attorneys) which responded, **reported experiencing information security breaches.**

The Daily Advisor
March 2017

Bank Customers Hit by Problems with a Financial Service Provider
Tens of thousands of a bank's customers were impacted by problems **resulting from a hacking issues with a third party service provider** which processed payments between financial institutions.

TTG Media
March 2017

A healthcare company rushed to reassure nearly 43,000 individual members who were potentially affected by the data hack of a web server managed through a third party web developer and hosting company.

DataBreaches.net
March 2017

Patients notified of Data Breach
A janitorial vendor erroneously placed a healthcare provider's patients' protected health information (PHI) in the trash dumpster.

Recent Ponemon Institute surveys reveal:

- Unsecure third parties including cloud providers are seen as one of the top three threats to an organization.
- 41% of the companies surveyed experienced a data breach caused by a third party. And the consequent loss of brand value typically ranged from $184 million to more than $330 million
- 51% of companies surveyed experienced an average of 4 ransomware attacks and paid an average of $2,500 per attack

ERM Enterprise Risk Management Symposium

Third Party Risk Management Process

Establish Third Party / Contract Risk	Ensure Use and Completion of Due Diligence Activities and Control Assessments	Standard Contract Language	Formalize Oversight and Monitoring	Exit Strategy and Asset Return
Third Party • New/existing • RFx/sole source/renewals • Ethical Sourcing • Relationship owner is key **Risk Criteria** • Simple, clear and consistent • Applied at contract level • Due diligence requirements **Control Assessments** • Areas to include: security, information, personnel, site, business continuity, regulatory requirements, compliance, insurance, … • Leverage industry standards • Capture appropriate documentation **Remediation/Issue Closure**	**Clauses (Legal Approved)** • Right to audit • Information security • Physical security • Background checks • Business resiliency/disaster recovery • Fourth parties • Encryption requirements as appropriate • Termination and exit **Authorized Negotiators/Signers** • Goods and services • Specialized services (real estate, benefits, legal, etc.) **Exceptions and Approval**	**Leverage** • Assigned risk ranking • Assessments and prior reviews **Ongoing Monitoring** • Periodic validation of risk ranking • Frequency based on risk and service provided • Agree on scope and type of review to be performed • Perform onsite reviews • Point in time assessment move toward continuous monitoring **Remediation/Issue Closure** **Third Party Performance** • Scorecard program • Reporting **Software and License Compliance**	**Termination** • Normal • Cause • Convenience • Breach **Asset Return** • Return and/or confirmation of destruction of confidential data **Exit Strategies** • Developed internally, not with third party • Outlines approach to be followed if critical third party relationship prematurely terminates • Outlines various options to ensure continued availability of services	

ERM Enterprise Risk Management Symposium