You’ve Been Breached. Now What?

Sarah Ference, CPA
Risk Control Director, Accountants Program
CNA

Gregory J. Bautista
Attorney
Wilson Elser Moskowitz Edelman & Dicker LLP
The purpose of this presentation is to provide information, rather than advice or opinion. It is accurate to the best of the presenters’ knowledge as of the date the presentation was developed. The information, examples and suggestions presented in this material have been developed from sources believed to be reliable. Accordingly, this presentation should not be viewed as a substitute for the guidance and recommendations of a retained professional and should not be construed as legal or other professional advice. In addition, CNA does not endorse any coverages, systems, processes or protocols addressed herein unless they are produced or created by CNA. CNA recommends consultation with competent legal counsel and/or other professional advisors before applying this material in any particular factual situations. Any references to non-CNA Web sites are provided solely for convenience, and CNA disclaims any responsibility with respect to such Web sites. To the extent this presentation contains any examples, please note that they are for illustrative purposes only and any similarity to actual individuals, entities, places or situations is unintentional and purely coincidental. In addition, any examples are not intended to establish any standards of care, to serve as legal advice appropriate for any particular factual situations, or to provide an acknowledgement that any given factual situation is covered under any CNA insurance policy. Please remember that only the relevant insurance policy can provide the actual terms, coverages, amounts, conditions and exclusions for an insured. All CNA products and services may not be available in all states and may be subject to change without notice.

The AICPA Professional Liability Insurance Program is underwritten by one or more of the CNA insurance companies, and is administered by Aon Insurance Services.

“CNA” is a service mark registered by CNA Financial Corporation with the United States Patent and Trademark Office. Certain CNA Financial Corporations subsidiaries use the “CNA” service mark in connection with insurance underwriting and claims activities. Copyright © 2016 CNA. All rights reserved.
Learning Objectives

• Understand cyber liability risk and its impact on professional services firms, including CPA firms
• Understand how data breaches typically occur at professional services firms
• Understand the professional and legal responsibilities of a firm in the event of a data breach
• Understand the typical data breach response process and learn strategies to help ensure an appropriate breach response
• Gregory Bautista, JD
  – Lead member of Wilson Elser’s Breach Response Team and member of Accountants Practice Team
  – Focuses on data breach response, information governance and e-discovery
  – Represents clients in regulatory investigations

• Sarah Ference, CPA
  – Risk control director for CNA’s professional services customer segment
  – Oversees the delivery of risk management services to CNA customers in the professional services customer segment
Polling Question #1

What is your practice focus?

a) Tax advice/return preparation
b) Audit/attestation
c) Family office/business management/consulting
d) Other (not in public practice)
THE LANDSCAPE
What is Cyber Liability?

• Privacy – data and location tracking privacy expectations
• E-Publishing in the social media context
• Technology errors and omissions
  – Shared applications and data
  – Project management disconnects
• And......data breaches
Aggressive Regulatory Environment

• Who is regulating?
  – Federal Trade Commission
  – Securities and Exchange Commission
  – Department of Health and Human Services/Office for Civil Rights
  – State regulators
  – Foreign and international regulatory activity – Investigations of U.S. incidents
  – Federal Communications Commission

• Why?
  – Public attention
  – Media attention
  – Revenue generation
Polling Question #2

How many states have enacted breach notification statutes?

a) 10  
b) 34  
c) 47  
d) All of them
• 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring private or governmental entities to notify individuals of security breaches of information involving personally identifiable information
  – The holdouts – New Mexico, South Dakota, Alabama

• Typical provisions include:
  – Who must comply with the law
  – Definitions of “personal information”
  – What constitutes a breach
  – Requirements for notice exemptions

State Attorney Generals

- Trained by federal regulators in cybersecurity enforcement
- Use the same “play book” as federal regulators
- Maintain close communications with federal regulators and other Attorneys General
- Seek and use publicity effectively (e.g. California AG)
- Coordinate investigations
The allegations:
- Violation of privacy laws and common law rights
- Breach of contract
- Negligence
- Fraud
- Unfair trade practices

Alleged damages:
- Compensatory damages, treble damages, attorneys fees, punitive damages, civil monetary fines

Plaintiffs use regulatory fines as evidence of wrongdoing
• Protection of confidential client information is required by ethical standards and applicable laws, rules and regulations
  – AICPA Code of Professional Conduct, §1.700.001, Confidential Client Information Rule
  – State board of accountancy rules
  – Internal Revenue Code §7216
MORE ABOUT DATA BREACHES
• In 2015, U.S. data breaches tracked hit a near record high of 781 (flat to 2014 and 27% increase over 2013)
• Since 2005, 5,810 reported data breach incidents; 169 million estimated records exposed in 2015 breaches
• Industries affected in 2015:
  – Business services – 39.9%
  – Medical/healthcare – 35.5%
  – Banking/credit/financial – 9.1%
  – Government/military – 8.1%
  – Educational – 7.4%

What is a Breach?

• Definition
  – Access v Acquired - what does this really mean
  – Confidentiality, integrity, and security of the personal information - "risk of harm"
  – Encryption "safe harbor" - or is it?

• And don’t call it a “breach”
  – Legal impact of a "breach"
  – So what do you call it?
Polling Question #3

Has your organization/firm ever experienced a data security event?

a) Yes
b) No
c) Not sure
SO WHAT HAPPENS NEXT?
Life Cycle of a Breach

**Identification**
- Identify that an event has occurred and determine who should be involved
- Trigger the Incident Response Team

**Containment**
- Stop the bleeding – but don’t damage the wound!

**Remediation**
- Take steps to prevent a similar event from occurring in the future

**Notification**
- Who do you tell?
- How?
- When?
Who Ya Gonna Call?

- Data breach coach
- Forensic support
- IT support
- Public relations
- Insurance company
According to the Identify Theft Resource Center, what was the primary cause/type of breach in 2015?

a) Employee error/negligence
b) Hacking/skimming/phishing
c) Subcontractor/third party
d) Accidental exposure

AN OUNCE OF PREVENTION IS WORTH A POUND OF CURE
1. Assess

2. Address

3. Plan and Insure

4. Repeat

Leadership & Ownership
Leadership & Ownership

• Protecting client data is everyone’s responsibility
• But…it all starts with the tone at the top
  – Allocation of resources
  – Model the way
• Do you:
  – collect, store, or transact any personal, financial or health data?
  – transport sensitive or protected data on portable devices or paper files?
  – outsource computer network operations, data or network management?
  – share data with business partners or vendors?
  – have a website hosted on a shared server?
  – schedule recent and routine cyber risk assessments?
  – have encrypted electronic devices?
  – have current intrusion detection software/protocol?
  – have a posted privacy policy which aligns with your internal data management practices?

• How long do you maintain records?
Address the Risk

- **Policies and procedures**
  - Industry-specific requirements (HIPAA, for example)
  - Information security program
  - Access management
  - Password policy

- **Training and education**
  - Who?
  - How often?

- **Incident Response Plan**
  - Don’t wait until it’s too late
  - Living document – take it off the shelf and practice!

- Don’t forget about vendors!
• Mind the gap
  – Commercial general liability
  – Property
  – Professional liability
  – First party

• Information risk coverage – what to look for:
  – General terms and conditions
  – Third party coverages – network damage, privacy injury, event expenses, regulatory proceedings and extortion
  – First party coverages – business interruption and data restoration
• Monitor compliance
  – Employees
  – The firm itself
  – Vendors

• Hit refresh
  – Periodically update policies and Incident Response Plan to address changes in risk profile or regulations
What’s the first thing you will do after today’s webinar?

a) Google “Incident Response Plan” so I can get started on mine.

b) Call a coach – I need help!

c) Hide in a corner – I’m spooked.

d) Nothing. Got it covered.
QUESTIONS?
Wilson Elser's Data Privacy & Security and Technology teams help companies prepare, strategize and respond to risk management issues and data security events arising from cyber attacks that represent varying degrees of potential disruption, expense and reputational damage to companies.

Wilson Elser excels at advising our clients so they can anticipate these threats, prepare for the potential consequences, and respond quickly and effectively if and when attacks materialize. We offer services to assist with all aspects of cyber risk management, including the oversight of data and privacy assessments; development of incident response plans and policies and procedures; and assistance with implementation, training and testing of revised and existing plans and operations. Faced with an incident, our experienced breach coaches stand beside our client to navigate the overall response, including overseeing the investigation process, providing legal counsel to assist with compliance with federal and state legal notification requirements, assisting with development of appropriate responsive and remedial measures, and representing the client in connection with regulatory investigations.

Should an event result in litigation, our seasoned litigators can provide effective and collaborative defense strategies to help contain the risk and the ultimate impact of a data security event.

www.wilsonelser.com
CNA is the 8th largest U.S. commercial property and casualty insurance company¹. Founded in 1897, CNA has approximately 7,000 employees, serving businesses and professionals in the U.S., Canada, Europe and Asia. CNA products and services are sold by highly regarded independent agents and brokers.

At CNA, we focus on what we do best — providing insurance solutions that allow our customers to better manage their risks and grow profitably. We use our expertise to continually evolve our products and services to anticipate and address our customers’ needs. Our broad portfolio enables us to respond to a wide range of business risks while focusing on the specialized needs of our customer segments, including the professional services segment which serves the needs of accountants, lawyers, architects and engineers, real estate agents and other providers of professional services.

CNA is the number one provider of professional liability coverage for architects, engineers, contractors, attorneys, real estate agents and accountants. In addition, CNA provides a range of property and general liability coverage, which professionals need to manage the risk of running their business, from Professional and Cyber Liability to Employment Practices Liability and Workers’ Compensation.

¹Based on 2013 net written premium, A.M. Best.

www.cna.com
• **Legal Holds in Response to Data Breaches**, DRI: In House Defense Quarterly, Summer 2015

• **Third Circuit Holds FTC Has Authority to Regulate Cybersecurity under Unfairness Prong of 15 U.S.C. §45(a)**, Wilson Elser Client Alert, September 2015

• **The IRS will not flag, identify or otherwise note a SSN that may be subject to identity theft and subsequent tax fraud. Go figure.**, Professional Liability Advocate, June 2014

• **Surf’s Up: The Wave of High-profile Privacy Class Actions**, Professional Liability Advocate, July 2014
• Professional Liability Risks Related to Cloud Computing
• Protect Your Firm Against Data Security Breaches
• A Possible Privacy Breach: What Next?
• A Breach of Client Data: Risk to CPA Firms, Journal of Accountancy, August 2013
• Data Security Risk: You Can Take it Anywhere, Journal of Accountancy, April 2014
• Keeping your Computer Safe
Thank You!
Contacts

Gregory J. Bautista
Partner
White Plains, New York
914-872-7839
gregory.bautista@wilsonelser.com

Sarah Ference
Risk Control Director
Chicago, Illinois
312-822-3354
sarah.ference@cna.com