Cybersecurity and Data Privacy in Business Transactions

July 10, 2014

Stephen Stein,
Partner

Rose Romero,
Partner

Mike Titens,
Partner

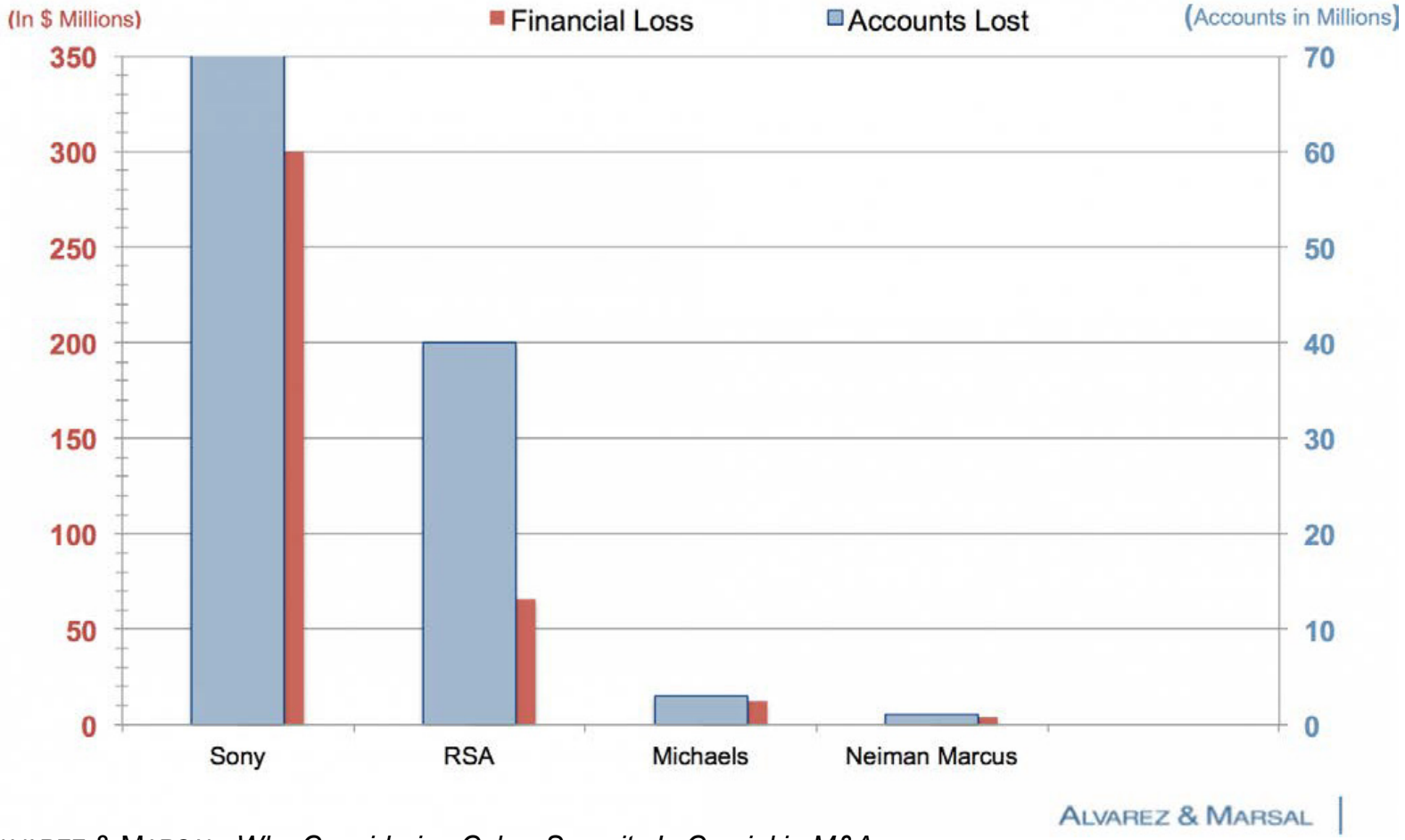
Craig Carpenter,
Associate

Data Breaches: By the numbers

- 42% increase in attacks in 2012*
- 102 successful attacks per week*
- The average cost of a data breach rose 15 percent since 2012 to $3.5 million per breach in 2013**
- The average cost paid for each lost or stolen record that contained sensitive and confidential information also increased by more than 9 percent, from $136 (2013) to $145**

*Ponemon Institute Research Report, 2013.
**ALVAREZ & MARSAL, *Why Considering Cyber Security Is Crucial in M&A Transactions* (June 25, 2014).

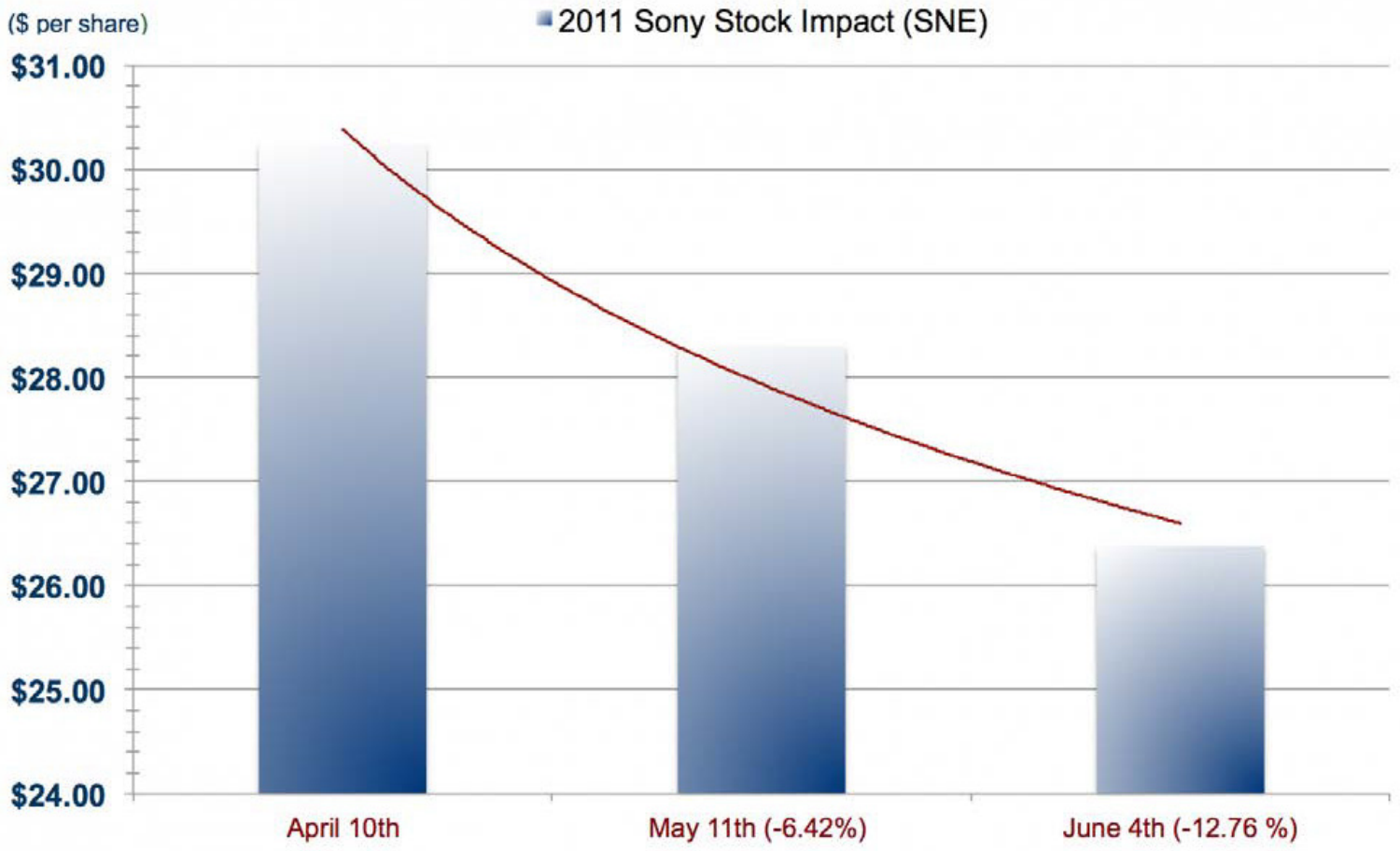
Costs of Data Breach



Source: ALVAREZ & MARSAL, *Why Considering Cyber Security Is Crucial in M&A Transactions* (June 25, 2014) (used with permission).

Thompson & Knight Impact
ATTORNEYS AND COUNSELORS

Costs of Data Breach



Source: ALVAREZ & MARSAL, *Why Considering Cyber Security Is Crucial in M&A Transactions* (June 25, 2014) (used with permission).

ALVAREZ & MARSAL

Thompson & Knight Impact
ATTORNEYS AND COUNSELORS

Cybersecurity Considerations in Business Transactions

- Cybersecurity and Data Privacy in M&A
- Data Protection in Service Agreements
- Increased Data Protection Regulation by the SEC
- Privacy and Data Protection Online

Cybersecurity and Data Privacy in M&A

Cybersecurity in M&A Transactions

When to Address Cybersecurity in the M&A Transaction:

- Due Diligence:
  - Review of privacy policies
  - Review of third party data
  - Review of vendor agreements related to cybersecurity
  - Review of Prior incidents & audits
- Transaction:
  - Reps & Warranties
  - Indemnities

Cyber Security and Privacy Due Diligence:

- Identify:
  - Types of data
  - Data sources/locations
  - Data collection processes
  - Supply chain risk
  - Prior incidents
  - Cybersecurity policies/agreements

Cybersecurity in M&A Transactions

Cybersecurity and Privacy in Transaction Documents:

- Compliance with privacy laws and data security standards
- Identification of data
- Cleansing
- Audit

Cybersecurity and Data Protection in Service Agreements

Cybersecurity – Service Agreements

- Agreements with vendors/contractors collecting, storing or processing data
- Vendors to whom you have outsourced functions dealing with data:
  - Data Centers
  - Marketing Firms
  - Credit Card Processors
  - IT Service providers

Cybersecurity in Service Provider Agreements

- Agreements that commonly involve cybersecurity and data protection issues
  - Hosting Agreements
  - Data Center Agreements
  - Cloud Computing Agreements
  - SaaS Agreements
  - Outsourcing Agreements
  - Services Agreements (data processing, transmission, development, etc.)

Cybersecurity in Service Provider Agreements

- Have procedures and contract provisions in place to:
  - Limit use of data/networks
  - Have data returned to you
  - Have data transferred to a subsequent service provider
  - Have data destroyed
- Agreements should also address:
  - Minimum standards
  - Breach notification
  - Auditing
  - Liability/indemnification/remedies
  - Insurance coverage

Cybersecurity in Service Provider Agreements

- Data Protection Standards – set out minimum requirements for:
  - Physical Security
  - Technical Security
  - Administrative Security

SEC Cybersecurity Regulation

SEC's New Focus on Cybersecurity

1. Cybersecurity Guidance, Division of Corporation Finance – October 2011
2. SEC Risk Alert and Cybersecurity Initiative – April 2014

Cybersecurity Issues and the SEC

"[B]oards that choose to ignore, or minimize, the importance of cybersecurity oversight responsibility, do so at their own peril."

SEC Commissioner Luis Aguilar
New York Stock Exchange Conference

The SEC's Cybersecurity Guidance

Disclosure of Cybersecurity issues under Reg S-K

- Six areas where disclosure may be necessary
  1. Risk Factors
  2. MD&A
  3. Description of Business
  4. Legal Proceedings
  5. Financial Statement Disclosures
  6. Disclosure Controls and Procedures

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

DIVISION OF
CORPORATION FINANCE

May 18, 2012

We have reviewed your filing and have the following comments. In some of our comments, we may ask you to provide us with information so we may better understand your disclosure.

1. We note that none of your risk factors, or other sections of your Form 10-K, specifically address any risks you may face from cyber attacks, such as attempts by third parties to gain access to your systems to compromise sensitive business information, to interrupt your systems or otherwise try to cause harm to your business and operations. In future filings, beginning with your next Form 10-Q, please provide risk factor disclosure describing the cybersecurity risks that you face or tell us why you believe such disclosure is unnecessary. If you have experienced any cyber attacks in the past, please state that fact in any additional risk factor disclosure in order to provide the proper context. Please refer to the Division of Corporation Finance's Disclosure Guidance Topic No. 2 at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm for additional information.

SEC Cybersecurity Priorities

- Initiative to assess cybersecurity preparedness in the securities industry
- 28 “sample” information requests sent to 50 firms
- Information requests incorporate the National Institute of Standards and Technology (NIST) cybersecurity framework published in February 2014

Cybersecurity Checklist

- The entity's cybersecurity governance
- Identification and assessment of cybersecurity risks
- Protection of networks and information
- Risks associated with remote customer access and funds transfer requests
- Risks associated with vendors and other third parties
- Detection of unauthorized activity
- Experiences with certain cybersecurity threats

Privacy and Data Protection Online

Privacy and Data Protection Online

- Website privacy policies and terms of use are becoming more significant due to:
  - Increased FTC enforcement
  - Recent State Regulations and Enforcement
  - Strict EU Regulations
  - Canada Anti-spam Laws
- Privacy policies and terms of use should be accurate and up-to-date.

Questions or comments:

Stephen Stein	Rose Romero	Mike Titens	Craig Carpenter
Partner,	Partner,	Partner,	Associate,
214-969-1209	214-969-2500	214-969-1437	214-969-1154

Additional Information:

http://www.tklaw.com/data-privacy-and-cybersecurity/

http://www.tkcybersecurityblog.com/