Stock & Option Solutions

Data Do's and Don'ts: How to Keep Your Employee Data Safe

HF J&A

HOGE FENTON
Hoge Fenton Jones & Appel
Attorneys at Law | Founded in 1952

Solium

Today's Speakers

Pam Ellis, CEP

VP, Communications & Industry Relations

Solium Capital, LLC

Barrett Scott

Principal & Co-Founder

Stock & Option Solutions, Inc.

Stephanie Sparks

Attorney, IP Group Chair

Hoge Fenton Jones & Appel

Disclaimer

The following discussion and examples do not necessarily represent the official views of Stock & Option Solutions, Inc., Solium Capital, or Hoge Fenton Jones & Appel with respect to any of the issues addressed. Moreover, this presentation and the views expressed by the individual presenters should not be relied on as legal, accounting, auditing, or tax advice. The outcome of any individual situation depends on the specific facts and circumstances in which the issue arises and on the interpretation of the relevant literature in effect at the time.

Anyone viewing this presentation should not act upon this information without seeking professional counsel and/or input from their advisors. Transmission of the information is not intended to create, and receipt does not constitute, an attorney-client relationship.

Agenda

- Personal Identifying Information (PII) Defined
- The Dark Side of PII Management
- PII and the Equity Data Life Cycle
- Assessing Weakness in the Cycle
- Assessing the Risks
- Action Plan to Strengthen Your Data Security
- Recommendations

Personal Identifying Information (PII)

- *Generally* includes individual's first name or first initial and last name in combination with any one or more of the following:
  - Social security number;
  - Driver's license or identification number; or
  - Account number, credit or debit card number, in combination with any required security code, access code or password

  OR
  - Medical or health insurance information (not covered in this presentation)

The Dark Side of PII Management

- 50% of data breaches caused by a stolen/lost laptop
  - A laptop is stolen every 12 seconds
  - 88 % employee negligence
  - 44 % third-party mistakes (e.g., your copy vendor)
  - 5 % employee theft
  - 95 % of employee theft cases involve IT personnel

Sources: Open Security Foundation, datalossdb.org; Ponemon Institute, ponemon.org

Other Types of Data Breaches

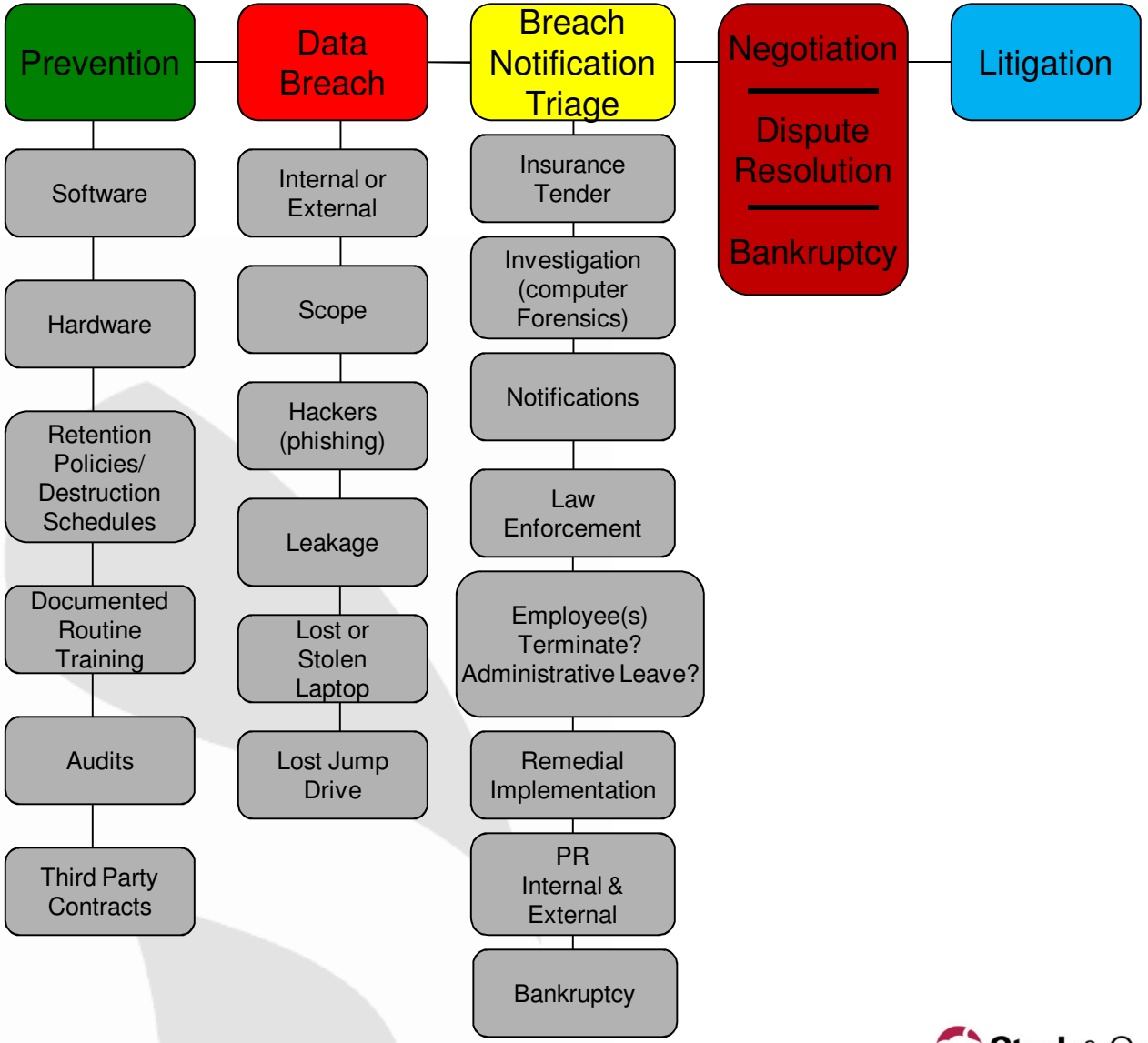
- Lost or stolen computers or storage devices
- Inadvertently including PII on mail merged envelope labels
- Employees rummaging through files
- Unsealed envelopes in the mail
- Tossing PII without shredding
- Private data left on copier buffers
- Phishing
- Malware (Rootkits, Botnets, Viruses, Worms, Spyware)
- Credit card “knuckle scraper” papers

The Cost of a Data Breach

- 509 million records were compromised in last three years (2008 – 2010)
- A typical lost or stolen laptop cost a business an average of $50,000 due to data breach
- Range of loss to the individual: $1,213 to $975,527

Sources: 2011 Verizon Data Breach Investigation Report; Open Security Foundation, datalossdb.org; Ponemon Institute, ponemon.org

Lifecycle of Data & the Security Breach



Stock & Option Solutions

The Patchwork of Laws

- Key federal laws
  - Gramm-Leach-Bliley Act (GLBA regulated by FTC)
  - Federal Credit Reporting Act (FCRA regulated by FTC)
  - Fair & Accurate Credit Transactions Act and Red Flags Rules (FACTA regulated by FTC)
  - Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act) (regulated by HHS)
  - The Children's Online Privacy Protection Act
  - The Communications Decency Act
  - Foreign Intelligence Surveillance Act (FISA)
  - Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM)
  - Federal Identity Theft and Assumption Deterrence Act

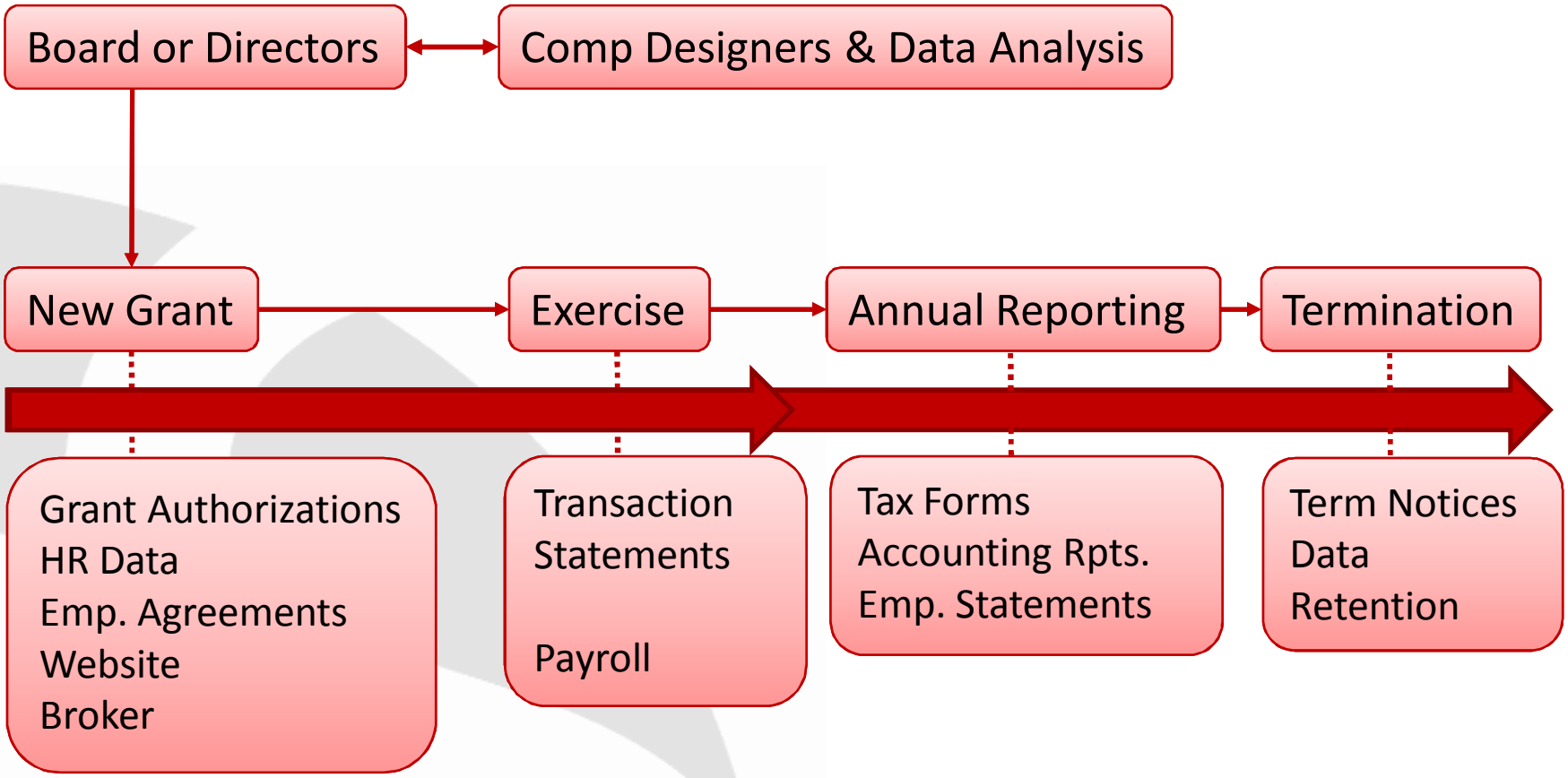
The Patchwork of Laws (cont'd)

- State laws
  - Most stringent: Massachusetts
  - 47 states and the District of Columbia
  - 9 states added laws within last three years: Alaska, District of Columbia, Iowa, Missouri, South Carolina, Virginia, West Virginia, Iowa, Mississippi

State Data Security Breach Notification Laws

- Notice requirements *generally* include:
  - Data custodian to (i) data owner
  - Data owner to (ii) affected resident and (iii) possibly State Attorney General
  - Timing:
    (i) "immediately following discovery of the breach"
    (ii) "most expedient time possible and without unreasonable delay"

PII and the Equity Data Life Cycle



Assessing Weaknesses in the Data Cycle

- **People**
  - Accident, negligence, fraud
- Location
  - Paper, laptop, servers, websites, system backups
- Data in transit
  - Email, hardware, between systems over Internet
- Vendors

Assessing Weaknesses in the Data Cycle (cont'd)

- Access: how, who and when
  - Hardware system
    - Files systems
  - Software system (website or database)
  - Email system
- **People, People, People**
  - **Educate, Educate, Educate**

Assessing the Risks

- How to prioritize the level of risk?
  - What data is available?
  - Who could possibly get it?
  - What happens if data is accessed by the wrong people?
  - Is someone responsible for standard of care of protecting this data?

Risk Matrix

Identified Risk	What is at risk?	Who could get it?	Where could it go?	Responsible Person Identified	Total
Printer/Copier	1	1	1	5	8
Internal Manual Email with HR Employee Export w/SSN	5	1	1	3 (sender)	10
Un-Encrypted Laptop	5	5	5	5	20
Employee Internet Based Website	5	5	5	1 (IT Security)	16
Vendor Data Transmission	5	5	5	3	18

Rank 1 is low risk – 5 is high risk

Assessing the Risks (cont'd)

- What controls do you have in place?
  - Locked-down technology
  - Preventative policies
    - "Don't do this" rules
    - Education
  - Detective procedures to identify issues
    - Controls in place
- Risk mitigation
  - Insurance and balance sheet

Action Plan to Strengthen Your Data Security

- How can technology help you?
  - Learn how system security can segregate data from users in all systems
  - Encryption, user access controls, audit trails
- How can standard processes help you?
  - Define “the way we do it here!”
  - Learn from other departments
  - SOX Controls
  - ISO/IEC 27000 series of standards

Action Plan to Strengthen Your Data Security (cont'd)

- Security Audits
  - 3rd party Audit
  - Insurance may require
  - Security Questionnaire (ISO/IEC 27002)
- Vendor review and questionnaire
  - SSAE 16 (replaced SAS 70)
  - Security questionnaire (ISO/IEC 27002)

Assessing Your Vendor

- What questions to ask?
  - Info Sec dept can provide questions based on ISO 27002 or other standard
  - Help with review of SSAE 16
- What should you expect?
  - Openness and cooperation
- Why would they not share in more detail?
  - Part of security is not knowing…..

Assessing Your Vendor (cont'd)

- Legal review of vendor
  - Contract representations and warranties
  - Limitations of indemnity and damages
- What is acceptable risk with vendors?
  - Do you have other solutions available?
  - What is the plan for the vendor to perform risk mitigation?
  - What happens if you identify unacceptable risk?
- Use this process to become educated on Security issues

Who is Responsible for Data Protection?

- Management: is this culturally important?
- Every employee
- Steps to increase priority of the issue
  - Matrix – proof is issue
  - Do you have corporate allies and champions?
  - Can you make corporate allies?
- What teams/people need to be at the table?
  - Are they motivated to move this forward?

Recommendations

- What can you influence?
  - Be honest
  - You can do more than you think!
  - You can limit who sees the data
- Education
  - What, Who, Risk, Responsibility, Action Plan
  - Employee agreements
  - Ongoing education plan, not just one time
  - If they don't know the importance, you're bound to fail

Recommendations (cont'd)

- Plan for worst case scenario (hope for the best)
  - Create procedures
  - Response plans
  - Practice - fire drills
- There is no perfect answer
  - When assessing solutions, give yourself choices of ways to reduce the risk
  - Don't have only one way to resolve a risk when choosing
- Look for Opportunity; Don't be driven solely by risk

The Inevitable Data Breach: 10 Tips

1. Use software and hardware firewalls **on all computers**
2. **Encrypt mobile and storage devices; encrypt data**
3. Don’t use peer-to-peer file sharing software
4. **Don’t use chat or IM software**
5. Install/update anti-malware software
6. Upgrade operating system
7. **Use up-to-date web browsers**
8. **Use/change strong passwords and store carefully**
9. **Beware of emails (unknown senders, phishing)**
10. **Educate and train employees**

Questions & Contact Information

Barrett Scott - Principal and Co-Founder
Stock & Option Solutions, Inc.
(408) 979-8708
bscott@sos-team.com
www.sos-team.com

Pam Ellis – VP, Communications & Industry Relations
Solium Capital LLC
(480) 308-8166
pam.ellis@solium.com
www.solium.com

Stephanie Sparks – Attorney, IP Group Leader
Hoge Fenton Jones & Appel
(408) 947-2431
sos@hogefenton.com
www.hogefenton.com