2016 ABA Annual Cyber Panel Presentation

Jeff Birnbach, Partner & Managing Director
Sylint Group, Inc.

Nora Wetzel, Associate
Sedgwick, San Francisco

Michelle Worrall Tilton
Media Risk Consultants LLC

August 5, 2016
Why Do I Care?

Data Breaches are Frequent and Costly

- Reputation
- Legally (lawsuits, regulatory sanctions)

43 million known security incidents in 2014
- 1.7 million daily attacks
- 48% increase

NY Attorney General reports data breaches are up by 40%

Vulnerability

- Intentional or accidental data releases
- Target or drive-by incidents
- Internal or external perpetrators
- Criminal or nation-state attackers

Every business, organization and entity is vulnerable - 100%

Damage & Harm

- Reputational harm
  - Shareholder value
- Extortion / Ransomware
- Regulatory compliance & notification costs
- Cost of monitoring
- Competitive advantage
- Network de-identification
Data Breaches are Frequent and Costly

- Reputation
- Legally (lawsuits, regulatory sanctions)

CA alone: 178 breaches affecting 24 million records

3 in 5 Californians victim of data breach
CA alone: 178 breaches affecting 24 million records
3 in 5 Californians victim of data breach
43 million known security incidents in 2014

- 117,000 daily attacks
- 48% increase

NY Attorney General reports data breaches are up by 40%

AT&T Cybersecurity Insight Report
Office of NY Ag Eric Schneiderman
Damage & Harm

- Reputational: brand - shareholder value
- Extortion / Ransomware
- Regulatory compliance & notification costs
- Credit monitoring
- Competitive advantage
- Network utilization (launching point)

[Incident is not Immediate]

Average period from initial incident to detection is 195 days!

But response must be timely.
Incident is not Immediate

Average period from initial incident to detection is 195 days!
But response must be timely.
Vulnerability

- Intentional or accidental data releases
- Target or drive-by incidents
- Internal or external perpetrators
- Criminal or nation-state attackers

Every business, organization and entity is vulnerable - 100%
Every business, organization and entity is vulnerable - 100%
Types of Breaches

Break it Down: CA 2015

58% Malware & Hacking
17% Physical Breach (thieves)
17% Errors
8% Other

Data Affected
Stolen Patient Records
Medical Care
1% of records
Stolen Personal Information

Cybersecurity Protects Intangible Assets

Top 20 Security Controls

Why do I care?

Data Breach
Firewall
User Education
Incident Response Plan
Financial Sector
Data Breach Stress Test

Break it Down:
CA 2015

58 percent
Malware & Hacking

17 percent
Physical Breach (theft/loss)

17 percent
Errors

8 percent
Other

Data Affected
- SSN: just under half of breaches
- Medical information: 19% of breaches
- What about financial information?
58 percent Malware & Hacking
17 percent
Physical Breach (theft/loss)
Errors
17 percent
Data Affected

SSN: just under half of breaches

Medical information: 19% of breaches

What about financial information?
Why do I care?

Retailers:
Growing focus on SSN theft given retailer transition to chip payment cards

Financial Sector:
2nd largest share of breaches

Healthcare:
16% of breaches
Cybersecurity Protects Intangible Assets

Top 20 Security Controls

Complex, but let's boil it down...

- Identify areas of highest risk and continuously assess and remediate critical vulnerabilities
- Maintain and monitor security (e.g., active directory) and edge (e.g., firewall) logs (Sentinel Collector)
- Develop and deploy application white listing on high-value targets (e.g., domain controllers)
- Add file integrity monitoring to critical files and application servers
- Monitor and secure outbound routes with the same discipline as inbound routes
- Centralize and increase frequency of patch management
- Develop a comprehensive system of scanning and identify sensitive information repositories
- Move highly sensitive management controls (e.g., SAN Management) off the enterprise network
- Build external segmentation
- Inventory and track all hardware and software (including (DHOD) inventory)
- Implement encryption into critical services and paths
- Centralize, track, and audit use of administrative privileges
- Limit users to least possible privileges
- Monitor and control account creation and termination
- Avoid (at least) distributed passwords (e.g., using the same "local admin" password)
- Limit and control remote access capabilities (e.g., VPD, ..., enhance authentication processes)
- Implement and test disaster recovery and business continuity plans
- Provide continuous security training for all employees/users
- Onboard and monitor incident response representatives and capability
- Test defense-in-depth concepts with penetration tests, and red teaming.

Why do I care?

Retailers:
Growing focus on SSN theft given retailer transition to chip payment cards

Financial Sector:
2nd largest share of breaches

Healthcare:
16% of breaches
Cybersecurity Protects Intangible Assets

COMPONENTS of S&P 500 MARKET VALUE

SOURCE: OCEAN TOMO, LLC
*JANUARY 1, 2015
Top 20 Security Controls

Complex, but let's boil it down...

- Identify areas of highest risk and continuously assess and remediate critical vulnerabilities
- Maintain and monitor security (e.g., active directory) and edge (e.g., firewall) logs (See Log Collection)
- Develop and deploy application white-listing on high value targets (e.g., domain controllers)
- Add file integrity monitoring to all public-facing and application servers
- Monitor and secure outbound routes with the same discretion as inbound routes
- Centralize and increase frequency of patch management
- Develop information classification processes and Identify sensitive information repositories
- Move highly sensitive management controls (e.g., SAN Management) off the enterprise network
- Build internal segmentation
• Inventory and track all hardware and software (including BYOD)
• Implement encryption into critical services and paths
• Control, track and audit use of administrative privileges
• Limit users to least possible privileges
• Monitor and control account creation and termination
• Avoid identical distributed passwords (e.g., using the same "local admin" password)
• Limit and control remote access capabilities (e.g., VPN) ... enhance authentication processes
• Implement and test disaster recovery and business continuity plans
• Provide continuous security training for all employees/users
• Develop solid incident response processes and capability
• Test defense-in-depth concepts with penetration tests and red teaming
Data Breach Action Items

Incident Response Plan

- Incident Response Plan (IR) practical tips:
  - Team members’ phone numbers, backups
  - Card Processors, Vendors, Law Enforcement, Credit Monitoring Agencies
  - Update and test IR plan regularly and often
  - Use easy to follow checklists
   - Keep detailed logs (including evidence logs)
   - IT/MIS Personnel - CISO/CIO
   - Human Resources
   - Public Relations
   - Security - CISO/Chief Security Officer
   - Compliance
   - Risk/Insurance
   - External Cybersecurity/Forensics
   - Legal
   - General Counsel
   - Specialty Counsel - Breach Response, PCI, ISO 27001

Preparation

- Before a Security Incident / Data Breach:
  - Words matter: security incident vs. data breach
  - Have an incident response plan and follow it
  - Have a policy and follow it
  - Employee training
  - Inventory of data

- Current Trend = Pre-occupation with Security Tools

- Cohesive Cybersecurity Strategy is Critical:
  - Usually missing!
   - Understand value and importance of specific cyber assets
  - Prioritize resources in relationship to value
  - Deploying cybersecurity posture assessments

- Anticipate Incidents:
  - IR Team
  - IR Plan
  - IR WarGames

Basics to Prevent Breaches:

1. Monitor systems, usage, access, data, privilege
2. Limit access, risk, devices
3. Log events, breaches, servers, applications
4. Encrypt: data, passwords
5. Password: change, complex
6. Patch: systems, applications, devices

Do’s & Don’ts

- DON’T delay responding
- DO preserve ALL relevant data (logging, backups, hard drives)
- DON’T assume singular event
- DO engage outside investigators / forensics
- DON’T report prematurely
- DO communicate internally daily

What if you do not have an IRT?

- CALL ME! Get counsel involved
- Counsel should have tried and true checklist
- Additional resources
Basics to Prevent Breaches:

1. **Monitor**: systems, usage, access, data, people
2. **Limit**: access, privileges
3. **Log**: access, firewalls, servers, applications
4. **Encrypt**: data, passwords
5. **Password**: change, complex
6. **Patch**: op systems, applications, devices
Preparation

- **Before a Security Incident / Data Breach:**
  - Words matter: security incident vs. data breach
  - Have an incident response plan and follow it
  - Have a privacy policy and follow it
  - Employee training
  - Inventory of data

- **Current Trend > Pre-occupation with Security Tools**

- **Cohesive Cybersecurity Strategy is Critical:**
  - Usually missing!
  - Understand value and importance of specific cyber assets
  - Prioritize resources in relationship to value
  - Ongoing cybersecurity posture assessments

- **Anticipate Incidents:**
  - IR Team
  - IR Plan
  - IR Wargames

---

**Do's and Don'ts**

- **DON'T** delay
- **DO** preserve evidence
- **DON'T** assume it’s not us
- **DO** engage legal
- **DON'T** report incidents
- **DO** communicate

**What if we get hit?**

- CALL ME! Get in touch
- Counsel shocked employees
- Additional remarks
Preparation

- Before a Security Incident / Data Breach:
  - Words matter: security incident vs. data breach
  - Have an incident response plan and follow it
  - Have a privacy policy and follow it
  - Employee training
  - Inventory of data

- Current Trend > Pre-occupation with Security Tools
• Current Trend > Pre-occupation with Security Tools

• Cohesive Cybersecurity Strategy is Critical:
  • Usually missing!
  • Understand value and importance of specific cyber assets
  • Prioritize resources in relationship to value
  • Ongoing cybersecurity posture assessments

• Anticipate Incidents:
  • IR Team
  • IR Plan
  • IR Wargames
Incident Response Plan

- Incident Response Plan (IRT) practical tips:
  - Team members: phone numbers, backups
  - Card Processors, Vendors, Law Enforcement, Credit Monitoring Agencies
  - Update and test IRT regularly and often
  - Use easy to follow check lists
  - Keep detailed logs (including evidence logs)

- IT/MIS Personnel - CISO/CIO
- Human Resources
- Public Relations
- Security - LEO Coordination
- Compliance
- Risk / Insurance
- External Cybersecurity / Forensics
- Legal
  - General Counsel
  - Specialty Counsel - Breach Response, PCI, 50 State Notification
Do's & Don'ts

- DON'T delay responding
- DO preserve ALL relevant data (logging, backups, hard drives)
- DON'T assume singular event
- DO engage outside investigators / forensics
- DON'T report prematurely
- DO communicate internally daily

What if you do not have an IRT?

- CALL ME! Get counsel involved
- Counsel should have tried and true checklist
- Additional resources
Phases of Data Breaches

**Discovery / Investigation**
- What happened?
- What is affected?
- Control communications to the public
- Key players:
  - IT, Network Security or Information Security, Forensic Investigator, PR

**Containment / Assessment**
- Stop the bleeding
- Regulatory compliance: what laws apply (States, HIPPA, GLBA, ECPA)
- Compliance with contracts
- Key players:
  - Executives, employees, law enforcement and counsel

**Notice**
- What laws apply - regulatory compliance
- When to notify
- To whom:
  - Individuals
  - Government Agencies
  - Credit Monitoring Agencies
  - Media
- Contents of notice
- Method of notice
- Contractual notice
- When to notify
- To whom
- Contents of notice
Discovery / Investigation

- What happened?
- What is affected?
- Control communications to the public
- Key players:
  - IT, Network Security or Information Security, Forensic Investigator, PR
Containment / Assessment

- Stop the bleeding
- Regulatory compliance: what laws apply (States, HIPPA, GLBA, ECPA)
- Compliance with contracts
- Key players:
  - Executives, employees, law enforcement and counsel
Notice

- What laws apply - regulatory compliance
  - When to notify
  - To whom:
    - Individuals
    - Government Agencies
    - Credit Monitoring Agencies
    - Media
  - Contents of notice
  - Method of notice
- Contractual notice
  - When to notify
  - To whom
  - Contents of notice
Case Studies

1. PCI Breach
   - Initial investigation by a third-party determined
   - 90-day window
   - Credit card processed during period > 200,000
   - Court not satisfied; engaged lawyers to review
   - Identified means of attribution, specific costs
   - Reduced impacted cards < 10,000

2. Phishing Attack
   - Phishing email targeted users
   - Company fraud investigation
   - Cost of damage: $300,000 due to initial breach investigation
   - Card statements issued and fraud alert placed; follow-up calls and
   - Franked by bank for accounts with no activity
   - Phish cleaned from servers and account verified
   - Continues to monitor and learn from incident

3. Data Leak
   - Customer reviews they have heard company leaking data due to defective
   -認めなかった security vulnerabilities; affecting 25,000+ other customers
   - Timeline reconstructed and anti-forensic
   - Malware compromised user records; targeted
   - Identified that 5000+ users were impacted; notified and
   - Additional customer problems
PCI Breach

- Initial investigation (by others) determined 6 month window
- Credit cards processed during period >200,000
- Counsel not satisfied, engaged Sylint to review
- Identified means of exfiltration, specific cards affected
- Reduced impacted cards <20,000
2 Phishing Attack

- Phishing email grabbed user credentials
- Company forced password reset
- Counsel encouraged client to conduct broader investigation
- Sylint reviewed AD and firewall logs, identified foreign access
  - Promiscuous assignment of admin cred's
  - Intruders had established new admin accounts
  - Continued unauthorized access after reset
Data Leak

- Customer advises they have found company leaking data due to defective site coding, possibly impacting 20,000+ other customers
- Sylint reviews firewall and web logs, site coding
- Advises company on ways to secure data, terminate unauthorized access
- Identifies only 9 records were improperly accessed, all by the one initial customer reporting the issue
Insurance

According to the ABA, law firms generally spend less money securing their networks than other industries.

60% of small to medium sized businesses close within 6 months after sustaining a data breach.

Liability

Some Statistics

- Average data breach costs: $1.6 Million
- Average lost revenue: $3.4 Million
- Average number of records: 23,647
- Average cost per record: $201

Insurance Specifics

Final Thoughts
Insurance

According to the ABA, law firms generally spend less money securing their networks than other industries.

60% of small to medium sized businesses close within 6 months after sustaining a data breach.

Some Statistics

Average post data breach costs: $1.6 Million
Average lost business costs: $3.4 Million
Some Statistics

Average post data breach costs: $1.6 Million
Average lost business costs: $3.4 Million
Average records lost per breach: 23,647 Records
Average cost per record breached: $201 Per Record

Source: Ponemon Institute LLC
Insurance Specifics

Transferring Risk to Insurance
- Do not assume that there is coverage for network security
- Merit policies specifically exclude
- Must be endorsed to a professional liability policy, such as Attorney Professional Liability
- Are the limits adequate?
- Is there coverage for first party exposures?
- May need stand alone policy
- Utilize an experienced broker

Coverage Enhancements (Endorsements)
- Forensics (FP):
  - $5K to determine how the breach event happened
- Cyber Education (EP):
  - Data loss for ransom
- Regulatory Action Coverage:
- Defense coverage for responding to regulatory action
- Coverage for fines and penalties that may be imposed
- PCI fines/penalties:
  - Increasing fines for PCI compliance violations – $5K-$100K
  - More of a focus with high volume merchants
- Definition of "loss" does not include "fines or penalties"
- Business Interruption (IP):
  - Loss of business coming from network security failure (malicious code or loss of business from a system failure)
  - Insured must wait 8-12 hours before the interruption is on insurance event
- Contingent Business Interruption (IP):
  - Business interruption from failure of a third party cloud network

First Party Exposures
Losses Sustained by the Insured
- Consequence of network security failure
- Data breach, loss of information
- Control of remedies available
- Coverage of network security requirements
- Legal fees and penalties
- PCI audit to address any concerns of loss of good will
- Insurance payments for cyber solutions

Third Party Exposures
Losses Sustained (Claimed) by a Third Party
- Cross-Action litigation
- Payment card reissuance expenses
- Payment card fraud expenses
- PCI fines/penalties
- Identity theft
- Loss of client corporate information/IP lawsuits
- Emotional distress from invasion of privacy

Network Security Insurance Basics
What's Covered (The Insuring Agreement):
- Network Security and Privacy
- Media Liability
- Coverage Enhancements may be included or may need to be endorsed for additional premium
- May be sub-limited
- May include co-insurance
- May include separate self-insured retentions
First Party Exposures
Losses Sustained by the Insured

- Computer forensics expenses to identify the size and scope of a breach or loss of information
- Notification of affected individuals
- Credit monitoring after loss of social security numbers
- Regulatory fines and penalties
- PR Expense to mitigate bad press and loss of good will
- Ransomware payments for cyber-extortion
Third Party Exposures Losses Sustained (Claimed) by a Third Party

- Class-Action litigation
- Payment card reissuance expenses
- Payment card fraud expenses
- PCI fines/penalties
- Identity theft
- Loss of client corporate information/IP lawsuits
- Emotional distress from invasion of privacy
Transferring Risk to Insurance

- Do not assume that there is coverage for network security
  - Most policies specifically exclude
- May be endorsed to a professional liability policy, such as Attorney Professional Liability
  - Are the limits adequate?
  - Is there coverage for 1st party exposures?
- May need stand along policy
- Utilize an experienced broker
Network Security Insurance Basics

What's Covered (The Insuring Agreement):

- Network Security and Privacy
- Media Liability
- Coverage Enhancements: may be included or may need to be endorsed for additional premium
  - May be sub-limited
  - May include co-insurance
  - May include separate self-insured retentions
Coverage Enhancements (Endorsements)

- **Forensics (FP):**
  - $$$ to determine how the breach event happened

- **Cyber Extortion (FP):**
  - Data held for ransom

- **Regulatory Action Coverage:**
  - Defense coverage for responding to regulatory action
  - Coverage for fines and penalties that may be imposed

- **PCI Fines/Penalties:**
  - Levied by banks for PCI compliance violations - $5k-$100k
  - More of a risk with high volume merchants
  - Definition of "Loss" does not include "fines or penalties"

- **Business Interruption (FP):**
  - Loss of business arising from network security failure (malicious conduct) or loss of business from an unintentional system failure
  - Insured must wait 6-12 hours before the interruption is an insurance event

- **Contingent Business Interruption (FP):**
  - Business interruption from failure of a third party cloud network
Liability

Copyright Infringement from Iconic Images

- Media liability arising from online content to the public, such as the insured's website.
- Should be occurrence coverage trigger
- Named perils include:
  - Defamation, invasion of privacy, emotional distress, copyright and trademark
  - Covers defense costs and third party loss
  - Are punitive damages covered?

Media Liability Example: Any Issues?
Media Liability

- Media liability arising from online content to the public, such as the insured's website:
  - Endorse social media content!!
  - Should be occurrence coverage trigger
- Named perils include:
  - Defamation, invasion of privacy, emotional distress, copyright and trademark
- Covers defense costs and third party loss
  - Are punitive damages covered?
Copyright Infringement from Iconic Images


Republication of 9/11 photo posted on Fox Facebook page with #neverforget.

In denying Fox’s motion for summary judgment based on “Fair Use” defense, court determined that the image was commercial speech because it generated good will and promoted Fox programming.
Media Liability Example: Any Issues?
Final Thoughts

Exclusions
There are many:
- Bodily injury, but does not include emotional distress
- Collection of PI without permission
- Criminal acts
- Failure to have a privacy policy
- Insured v. Insured
- Infrastructure interruption outside of the insured's control (Yes, the Cloud)

The Underwriting Process
Risk Management is a must!
- Type of network
- Reliance upon third parties networking services
  - Do third parties contractually agree to defend and indemnify the insured for loss?
- What kind of data is collected?
  - Are credit cards processed?
  - How is data retained and destroyed?
  - How is data protected?
  - Loss history
Exclusions

There are many:
• Bodily injury, but does not include emotional distress
• Collection of PII without permission
• Criminal acts
• Failure to have a privacy policy
• Insured v. Insured
• Infrastructure interruption outside of the insured’s control (Yes, the Cloud)
The Underwriting Process

Risk Management is a must:
- Type of network:
- Reliance upon third parties networking services
  - Do third parties contractually agree to defend and indemnify the insured for loss?
- What kind of data is collected?
  - Are credit cards processed?
  - How is data retained and destroyed?
- How is data protected?
- Loss history