The Rise of Compliance-Driven Security
<table>
<thead>
<tr>
<th>Offices</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Key</th>
<th>Canada</th>
<th>United States</th>
<th>Europe</th>
<th>Central and Eastern Europe</th>
<th>Africa</th>
<th>Middle East</th>
<th>Asia Pacific</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Offices</td>
<td>● Calgary</td>
<td>● Atlantic</td>
<td>● Barcelona</td>
<td>● Accra</td>
<td>● Abu Dhabi</td>
<td>● Beijing</td>
<td>● Almaty</td>
</tr>
<tr>
<td>x Associate offices</td>
<td>● Edmonton</td>
<td>● Boston</td>
<td>● Berlin</td>
<td>● Algiers</td>
<td>● Amman</td>
<td>● Hong Kong</td>
<td>● Ashgabat</td>
</tr>
<tr>
<td>○ Facilities</td>
<td>● Montréal</td>
<td>● Chicago</td>
<td>● Brussels</td>
<td>● Bissau</td>
<td>● Beirut</td>
<td>● Shanghai</td>
<td>● Baku</td>
</tr>
<tr>
<td>● Associate firms</td>
<td>● Ottawa</td>
<td>● Dallas</td>
<td>● Frankfurt</td>
<td>● Bujumbura</td>
<td>● Doha</td>
<td>● Singapore</td>
<td>● Tashkent</td>
</tr>
<tr>
<td>+ Special alliance firms</td>
<td>● Toronto</td>
<td>● Kansas City</td>
<td>● Madrid</td>
<td>● Cairo</td>
<td>● Dubai</td>
<td>● Abu Dhabi</td>
<td>● Tripoli</td>
</tr>
<tr>
<td>● Vancouver</td>
<td>● Los Angeles</td>
<td>● Paris</td>
<td>● Istanbul</td>
<td>● Cape Town</td>
<td>● Kuwait City</td>
<td>● Manama</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>● Miami</td>
<td>● New Orleans</td>
<td>● Prague</td>
<td>● Casablanca</td>
<td>● Muscat</td>
<td>● Muscat</td>
<td>●</td>
</tr>
<tr>
<td></td>
<td>● New York</td>
<td>● Phoenix</td>
<td>● Warsaw</td>
<td>● Dar Es Salaam</td>
<td>● - Riyadh</td>
<td>● -</td>
<td></td>
</tr>
<tr>
<td></td>
<td>● San Francisco</td>
<td>● Short Hills</td>
<td>● Johannesburg</td>
<td>● Kigali</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Silicon Valley</td>
<td>● St. Louis</td>
<td>● Kampala</td>
<td>● Lagos</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>● Washington, DC</td>
<td>● London</td>
<td>● Nairobi</td>
<td>● Luanda</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Milton Keynes</td>
<td>● Maputo</td>
<td>● Lusaka</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Nairobi</td>
<td>● Maputo</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Mongolian</td>
<td>● Saldan</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Ulaanbaatar</td>
<td>● Ulaanbaatar</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Lhasa</td>
<td>● Lhasa</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Xining</td>
<td>● Xining</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Lhasa</td>
<td>● Lhasa</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Ulaanbaatar</td>
<td>● Ulaanbaatar</td>
<td>● -</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Overview

- InfoSec/Privacy Legal Framework
- Enforcement Trends
- Case Studies
  1. Adventures in HIPAA
  2. Payment Card Incident Scenario
  3. Working with Forensic Investigators
Takeaways

• Compliance Becoming Dominant Risk Driver
  • Lawyers in the Data Center are Here to Stay

• Compliance is not Security

• Ideas for Surviving Compliance-Drive Security
Brief History of Security/Privacy Law - Step Back

• US Constitution:
  • 3rd / 4th / 5th / 9th ("penumbra") Amendments - various privacy-related protections
  • 1st Amendment - protects freedom of speech, including commercial speech and corporate speakers

• EU Constitution
  • Privacy is an express right
  • Free speech does not hold higher standing than privacy
  • Heavily Influenced by WWII Experiences
Brief History of Security/Privacy Law - Federal

• Early Developments
  • Fourth Amendment
  • Invention of Telephone/Wire Communications
    • Protections for Snail Mail
    • Wiretap Act

• Federal Legislation
  • 1970s
    • Privacy Act
    • Fair Information Practices
    • FISA
    • FERPA
    • FCRA
    • Bank Secrecy Act
  • 1980s
    • VPPA
    • ECPA
    • OECD Guidelines
  • 1990s
    • TCPA
    • DPPA
    • HIPAA
    • COPPA
    • GLBA
    • EU DPD
  • 2000s
    • FACTA
    • CAN-SPAM
  • 2010s
    • SEC / Agencies
Brief History of Security/Privacy Law - Federal

• Trends:
  • Point solutions
  • Segmented, patchwork
  • No unified definitions or expectations

The most terrifying words in the English Language
Enforcement - FTC

- FTC - Section 5 Authority
  - Unfair/Deceptive Trade Practices
- Broad Exercise of Authority
  - FTC v. Wyndham Worldwide

FTC Security/Privacy Enforcement Actions

*Source: FTC*
Enforcement - HIPAA

- Recent Omnibus Rule
  - Broadened BAA Definition
  - Expanded Authority

- Largely reactive
  - Proactive Audit Program Expanding

*Source: OCR*
Brief History of Security/Privacy Law - State/Local

- CalOPPA - privacy policy requirements
- Anti-spyware - CA, others
- Data Destruction - 27+ States
- PCI/Card liability - MN
- Security - MA, CA
- Employer Social Media

- Breach Notification
  - CA (2003), Now 47+ states
  - Similar but not identical
  - Transaction Privacy (ZIP)
    - 16 States
  - Insurance Departments
    - NY DFS inquiries
    - CT Insurance Bulletin

State jurisdiction limited to the borders of the state (or at least their residents).

Practical application nationwide?
Growth of State/Federal Laws and Regulations

Chart Title

- Federal Laws
- State Laws
- Cumulative

ChoicePoint Breach

Enforcement - States

- Jurisdictional Hook = Breach Notification Laws
- Coordinated Multistate Task Force
  - Led by CT and IL
  - Very Active

![Reported Data Breaches](chart.png)

*Source: ID Theft Resource Center*
Brief History of Security/Privacy Law - Self-Regulatory

• Let industries set own rules
  • Enforceable by FTC under Section 5

• Various levels of success
  • NIST Cybersecurity Framework
  • NTIA Multistakeholder Processes
  • EU-US Safe Harbor Framework
  • TRUSTe
  • DMA / NAI / IAB
  • W3C Do Not Track

• PCI
  • Card Networks
  • Merchant Banks
  • Card Issuers

• Class Action Litigation
  • TCPA
  • VPPA
  • Song-Beverly/Credit Card Privacy
Smoke 'Em If You Got 'Em

• Basically, anyone with any regulatory authority is using it for cybersecurity/privacy

• InfoSec a regulated industry?
Risk - Breach Costs

• 2014 Ponemon Cost of Breach Study
  • $201 per breached record
  • Average $5 million+ over 2 years

• Card-related Breaches Trend Highest
  • PCI framework allows recouping costs

• Sample of high-cost breaches:
  • Heartland Payment Systems ~130m records
    • $140mm; $26mm legal fees
  • TJX ~45m records
    • $250mm
  • Global Payments - ~7m records
    • $96m
## Data Compromise Risk Analysis Framework

### Summary of Potential Risk Exposure Sources

<table>
<thead>
<tr>
<th>Potential Sources of Risk:</th>
<th>Est Cost Range</th>
<th>Statutory Breach</th>
<th>Potential Cost Accrual Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compromise, No Breach</td>
</tr>
<tr>
<td>Preliminary Investigation</td>
<td>$250,000 - $800,000</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Breach Notice</td>
<td>$381,550*</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Regulatory Investigations</td>
<td>$1,350,000 - $3,550,000</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Consumer Class Action Litigation</td>
<td>$1,925,000 - $4,050,000</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Card Issuer/Bank Litigation</td>
<td>$850,000 - $1,700,000</td>
<td>Y</td>
<td>?</td>
</tr>
<tr>
<td>AG or FTC Litigation</td>
<td>$450,000 - $850,000</td>
<td>Y</td>
<td>?</td>
</tr>
<tr>
<td>PCI Compliance</td>
<td>$9,100,000*</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

**MAXIMUM ESTIMATED EXPOSURE**

$14,306,550 - $20,431,550

*Costs are variable, based on number of affected individuals or payment cards.

**Total numbers could be lower, for example, if a class action lawsuit was disposed of on motion to dismiss.
Overview of Legal/Reg Framework - Review

• Compliance Becoming Dominant Risk Driver

• Lawyers in the Data Center are Here to Stay

• Compliance is not Security
Where Are We Headed?

Compliance Spiral of Doom

- Compliant, not Secure
- More Security Budget to Legal/Compliance
- Regulator Scrutiny
- Breach
Suggestions:

• Lawyers are not going away, learn to work with them

• Communicate, build relationships between key stakeholders
  • Ongoing working relationship, not just when emergencies
  • Cross-discipline information sharing, e.g. Data Governance Boards
  • Wargame, tabletop exercises (including legal/compliance)

• Acknowledge core competencies, use them appropriately
  • Lawyers don't know operational security, regardless of what they tell you

• Build security-focused security, map to compliance

• Good places to start: Incident Response, Vendor Management
Case Study

Adventures in HIPAA
Case Study - Adventures in HIPAA

• What is a Security Incident?

• HIPAA:

  • Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (45 C.F.R. 164.304)

  • Response and reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes. (45 C.F.R. 164.308(a)(6)(ii))

  • Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information… (45 C.F.R. 164.314(a)(2)(i)(C))
Case Study - Adventures in HIPAA

• So, under the literal reading of the rule you have to:
  • Identify and respond to, mitigate, document and report suspected or known unauthorized access, use, disclosure, modification, destruction, interference, whether attempted or successful.

• Have you identified, documented and reported your port scans today?
Case Study - Adventures in HIPAA

• But wait, that's not all!
  • Do you have a relationship with CMS?

• CMS definition from typical Computer Matching Agreement (based on NIST):
  • "Incident" means the act of violating an explicit or implied security policy, which includes attempts (either failed or successful) to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data;…
  • …shall report suspected or confirmed incidents affecting loss or suspected loss of PII within one hour of discovery…
Case Study - Adventures in HIPAA

• HIPAA:
  • The acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the rules] which compromises the security or privacy of the [PHI]… (45 C.F.R. 164.402)
  • Disclosure outside the rules is presumed a breach unless "low probability … [PHI] has been compromised based on risk assessment…

• CMS:
  • An incident becomes a breach when there is the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than unauthorized purpose have access or potential access to personally identifiable information or personal health information, whether physical or electronic.

• State Breach Notification (MN):
  • …unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of information… (MN Stat 325E.61)
Case Study - Adventures in HIPAA

• Is it a Security Incident?
  1. Vulnerability scans
  2. Brute force login attempts
  3. File transfer over public Wi-Fi
  4. Website vulnerable to Heartbleed
  5. Exploitation of web vulnerability, upload of code
  6. Patient spreadsheet exposed on public file server

**HIPAA:**
**attempted or successful** unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**CMS:**
the act of **violating an explicit or implied security policy**, which **includes attempts (either failed or successful)** to gain unauthorized access to a system or its data, unwanted disruption or denial of service, the unauthorized use of a system for the processing or storage of data.
Case Study - Adventures in HIPAA

• Is it a Breach?
  1. Vulnerability scans
  2. Brute force login attempts
  3. File transfer over public Wi-Fi
  4. Website vulnerable to Heartbleed
  5. Exploitation of web vulnerability, upload of code
  6. Patient spreadsheet exposed on public file server

**HIPAA:**
acquisition, access, use, or disclosure of [PHI] in a manner not permitted under [the rules] which compromises the security or privacy...

**CMS:**
loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than unauthorized purpose have access or potential access to personally identifiable information

**MN State Breach:**
Unauthorized acquisition of computerized data that compromises the security, confidentiality or integrity of information
Case Study - Adventures in HIPAA

• Sample HIPAA BAA Language on Incident Reporting:

  • ACME will report, no less than quarterly, any successful Security Incidents of which ACME becomes aware. Notice is hereby provided, and no further notice will be provided, for Unsuccessful Security Incidents.

  • “Unsuccessful Security Incidents” shall include, but not be limited to, pings and other broadcast attacks on Business Associate’s firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.

  • The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required.
Case Study - Adventures in HIPAA

Takeaways

• Incident and breach questions are very fact specific

• Short reporting timeframes (1 hour for CMS, BAAs typically a few days, MN "as soon as reasonably possible")

• Often not enough information to know for sure
  • E.g. limited logs
Case Study

Payment Card Incident Scenario
Case Study - Payment Card Incident Scenario

• Saturday, May 17:
  • Call from USSS - may be an issue at ACME.
  • Still gathering information, cannot share more at this time.

• Saturday, May 17:
  • Email from Bart Crabs, a well-known security blogger, asking ACME to confirm whether it had a breach.

• Sunday, May 18:
  • ACME hires Forensics 'R Us to investigate.
Case Study - Payment Card Incident Scenario

• Sunday, May 18:
  • USSS reference vague sources. Information "consistent with" POS breach.
  • Cannot identify scope or scale, little data but reliable sources.

• Monday, May 19:
  • No update by USSS.

• Tuesday, May 20:
  • News media reaches out to former ACME employees, asking about security issues.
Case Study - Payment Card Incident Scenario

• Wednesday, May 21:
  • River Bank calls, says Card Network has concerns based on Common Point of Purchase analysis
  • 257 cards used at 46 ACME stores were later used in fraudulent purchases.
  • Triggered by recently lowered CPP thresholds.
  • Other recent big breaches started out this way, hence the early warning.

• No new USSS information. Forensics has not found any indication of a breach.
Case Study - Payment Card Incident Scenario

• Thursday, May 22:
  • Bart Crabs publishes story reporting potential breach at ACME, based on "confidential sources."

• Thursday, May 22:
  • A bank tells USSS (who tells ACME) they suspected 220,000 fraudulent cards could be linked to ACME over 2-3 years.
  • Card Network contacted USSS with a report that two banks had analyses that might indicate data loss at ACME.
Case Study - Payment Card Incident Scenario

• Friday, May 23:
  • No new information from USSS.
  • Forensics has not found indications of a breach.

• Friday, May 23:
  • Letter from MN state AG requesting information on potential breach.

• Tuesday, May 27:
  • Card Network says they had a few CPP hits but "wouldn't go crazy." No special fraud rules for ACME, no longer investigating.
Case Study - Payment Card Incident Scenario

• Tuesday, May 27:
  • Forensics states that they have found no indication of a card breach "but the investigation is still ongoing."

• Tuesday, June 3:
  • Forensics investigation substantially complete.
  • Some malware found but no indication of card exfiltration.
Case Study - Payment Card Incident Scenario

• Lessons:
  • Media often gets ahead of the facts
  • Don't let yourself get ahead of the facts
  • Understand exactly what it is you know
  • Understand what you don't know
  • Be ready to act swiftly when you need to
  • Be patient when you don't need to act
Case Study -

Working with Forensic Investigators
On February 25, 2014, Lawyer & Lawyer LLP engaged Forensics to conduct a due diligence forensic investigation at ACME to determine whether there had been a data breach and/or data compromise.

During the course of this investigation, ACME requested that Forensics perform a separate analysis of an FTP server (‘ftp.acme.com’) located in the DMZ of ACME's Lake Wobegon, MN data center.

It should be noted that activities and findings related to this evidence were determined to be unrelated to the previous activities and analysis.
Our objectives for this investigation were as follows:

1) determine whether unauthorized usage or access by a dismissed employee occurred on the FTP server ‘ftp.acme.com’; and,

2) identify any suspicious files related to such usage.
Conclusion:

Based on Forensics's examination of the source evidence, there are indications of unauthorized use of, and possible file exfiltration from, the in-scope FTP server ‘ftp.acme.com’.

The evidence suggests that several of the indicators are derived from activities performed by a user account assigned to the dismissed employee ('eve01'), as well as from a user account this employee had access to ('root'), and possibly a third user account ('num02').
Conclusion:

Suspicious activities discovered included commands issued to:

1) establish SSH and Telnet connections to multiple external servers/domains, including one which is registered to the terminated employee, one known suspicious domain, and two non-domestic domains;

2) edit/delete/wipe files;

3) port scan/sniff;

4) exfiltrate files;

5) create FTP user accounts; and

6) create the unauthorized user account ‘account.name’.
Case Study - Working with Forensic Investigators

On February 25, 2014, Lawyer & Lawyer LLP engaged Forensics to conduct a due diligence forensic investigation at ACME to determine whether there had been a data breach and/or data compromise.

During the course of this investigation, ACME requested that Forensics perform a separate analysis of an FTP server ('ftp.acme.com') located in the DMZ of ACME's Lake Wobegon, MN data center.

It should be noted that activities and findings related to this evidence were determined to be unrelated to the previous activities and analysis.
Case Study - Working with Forensic Investigators

Our objectives for this investigation were as follows:

1) determine whether unauthorized usage or access by a dismissed employee occurred on the FTP server ‘ftp.acme.com’; and,

2) identify any suspicious files related to such usage.
Conclusion:

Based on Forensics's examination of the source evidence, there are indications of unauthorized use of, and possible file exfiltration from, the in-scope FTP server ‘ftp.acme.com’.

The evidence suggests that several of the indicators are derived from activities performed by a user account assigned to the dismissed employee (‘eve01’), as well as from a user account this employee had access to (‘root’), and possibly a third user account (‘num02’).
Case Study - Working with Forensic Investigators

Conclusion:

Suspicious activities discovered included commands issued to:

1) establish SSH and Telnet connections to multiple external servers/domains, including one which is registered to the terminated employee, one known suspicious domain, and two non-domestic domains;

2) edit/delete/wipe files;

3) port scan/sniff;

4) exfiltrate files;

5) create FTP user accounts; and

6) create the unauthorized user account ‘account.name’.
Case Study - Working with Forensic Investigators

• Lessons
  • Forensics should go through counsel - drafts can be privileged
  • Forensic reports should stick to the facts and avoid legal conclusions
  • Many FI's are very good at what they do, but keep them focused on what they do
Thank you

Andy Blair
Dentons US LLP
1221 Ave of the Americas
New York, NY 10020
USA

Questions?
andy.blair@dentons.com
@andyhblair
dentons.com/andy-blair