Lawyers Leading the Race to Cybersecurity

Insulating Your Organization from a Data Breach

August 2016
JIM ELLIOTT
Assistant Regional Director, Southwest Region
Federal Trade Commission

REBECCA PERRY, cipp/us/g
Director of Professional Services
Jordan Lawrence

JEFF C. DODD
Partner
Andrews Kurth LLP

MATTHEW G. NIELSEN
Partner
Andrews Kurth LLP
Employee Error Leading Cause of Data Breaches, New Survey Says

A company’s cybersecurity is only as strong as its weakest link.

“Employee error” turns out to be the most common reason for a data breach at companies, according to a new cybersecurity report released Wednesday by the Association of Corporate Counsel. This means the breach occurred as the result of a mistake the employee made, such as accidentally sending an email with sensitive information to someone outside the company.

http://www.acc.com/legalresources/resource.cfm?show=1416928
Most important thing you wish you had known before the breach

“That breaches can occur out of employee negligence and not just cunning hackers.”

“That some employees working from home are on their own unencrypted devices.”

“The extent to which personal information was being shared by email.”

“Full mapping of company data and data flows.”

“The importance of enterprise wide sense of responsibility.”

“Better understanding of the risk of fraud by third parties.”

“The amount of personal data maintained on servers.”
DATA BREACHES BY INDUSTRY

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Healthcare/Social Assistance</td>
<td>56%</td>
</tr>
<tr>
<td>Insurance</td>
<td>36%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>33%</td>
</tr>
<tr>
<td>Retail Trade</td>
<td>32%</td>
</tr>
<tr>
<td>IT/Software/Internet-Related Services</td>
<td>31%</td>
</tr>
</tbody>
</table>

*Industries with highest percentage shown

2015 ACC Foundation: State of Cybersecurity Survey - Key Findings
Boards that choose to ignore or minimize the importance of cybersecurity responsibility do so at their own peril.

--Luis Aguilar, SEC Commissioner (June 10, 2014)
Best Practices - Board Involvement

• Board meeting agendas should include time to review and discuss cyber security issues and resource allocation. Quarterly, at a minimum.

• At least one board member has specialized IT and/or cyber security knowledge.

• Board understands how security resources are managed and monitored.

• Assure there is direct reporting to C-Suite on key security risks. Preferably independent of the IT director.

• Assure appropriate cyber insurance has been obtained and is annually reviewed by risk management thereafter.
Where Do Counsel Fit In?

• Pre-Breach Risk Management: statutory and contractual requirements, best practices

• The Post-Breach Legal Landscape
  • Consumer and Employee Class Actions
  • B2B Litigation
  • Regulatory Investigations, Enforcement Actions, and Penalties

• The Role of Legal Counsel
REGULATORY LANDSCAPE IN U.S.
WHAT DO REGULATORS WANT TO SEE?

• Copies of policies and procedures governing privacy and security
• Evidence of education and awareness training, including attendance logs
• Risk assessments conducted by the company over a several-year period
• Risk mitigation plans and responses developed as a result of the risk assessments
• Vendor or business associate agreements in place regardless of whether third party caused breach
• Copies of disaster recovery and business continuity plans
• Records of past security incidents
• Incident response plans and testing
“Conduct cybersecurity risk assessments across the ENTIRE organization at least annually.”
START WITH AN ENTERPRISE WIDE PERSPECTIVE

Subject Matter Experts

Department Managers

Department Employees
Identify Discrepancies that Lead to Breaches

- **Mobile SME**: We have the ability to remote wipe or disable company devices.
- **HR Manager**: My employees only access company information on company devices.
- **HR Employee**: I access company information on company and personal devices.
bulkorder.ftc.gov
1 Storing information longer than necessary
MAP OUT YOUR INFORMATION

Data Map

- Record
- Where
- Media
- Business need
- Source
- Application
- Usage
- Movement
- Sensitivity
- Privacy
- Retention
- Classification
- Regulatory
- Storage
84% Save to Laptops or Tablets
20% Save to Flash Drives or DVDs
18% Save to Cloud Storage
6% Forward to Personal Email
GET RID OF OBSOLETE INFORMATION

Current Retention Compared to Best Practice

- 71% Retained Longer
- 48% Tagged with Sensitive Information
- In Line
- Shorter
- No BP
1. Storing information longer than necessary
2. Allowing default, easy-to-guess passwords
3. Failing to segment or restrict access to data
4. Failing to provide employee training & oversight
What policy?
1. Storing information longer than necessary
2. Allowing default, easy-to-guess passwords
3. Failing to segment or restrict access to data
4. Failing to provide employee training & oversight
5. Lack of third-party service provider oversight
VENDOR DUE DILIGENCE

• Third party risk responsible for majority of major breaches

• You can outsource certain functions, but you cannot outsource liability

• Ensure effective process for monitoring, reviewing and auditing vendors
  ✓ Require maintenance of appropriate safeguards
  ✓ Request comprehensive risk assessment at least annually
  ✓ Indemnification
  ✓ Immediate notification of breach
  ✓ Review changes to provision of services, including changes in policies and procedures

• Protective contractual provisions
ASSESS VENDOR PRACTICES ANNUALLY

YOUR COMPANY

Vendors

Vendor Experts
ASSESS VENDOR PRACTICES ANNUALLY
Vendor Summary | Cleveland Enterprises

PROJECT: 2015 Cleveland Vendor Assessment
MAIN CONTACT: Mike Jones (mjones@cleveland.com)
CONTRIBUTED ON: November 10, 2015
SERVICE PROVIDED: Cleveland Enterprises assists Pulaski Corporation with the records retention program that includes managing the retention schedule and sending hold notices to employees.

### SENSITIVE INFORMATION OBTAINED

<table>
<thead>
<tr>
<th>Banking/ Financial Records</th>
<th>Employee and HR Info</th>
<th>Social Security Numbers</th>
<th>Credit/ Debit Card Data</th>
<th>Medical/ Healthcare Info</th>
<th>Intellectual Property Assets</th>
<th>Confidential Personal Info</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>

### ACCESS TO CORPORATE INFORMATION

<table>
<thead>
<tr>
<th>Direct access to sensitive information</th>
<th>Direct access within corporate network</th>
<th>Indirect access within corporate network</th>
<th>Physical access within corporate facilities</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### RISK AREAS

- ACCESS CONTROL
- BUSINESS CONTINUITY
- COMPLIANCE
- CORPORATE NETWORK
- DESKTOP ADMINISTRATION
- DEVELOPMENT & ACQUISITION
- FILE SERVER BACKUP
- HUMAN RESOURCES
- INFORMATION SECURITY
- PHYSICAL SECURITY
- DATA CLASSIFICATION
1. Storing information longer than necessary
2. Allowing default, easy-to-guess passwords
3. Failing to segment or restrict access to data
4. Failing to provide employee training & oversight
5. Lack of third-party service provider oversight
6. Failing to take steps to investigate incidents
IF THERE’S A SUSPECTED INCIDENT

Discovery of a Data Breach

- Theft, loss, or Unauthorized Disclosure of Personally Identifiable Non-Public Information or Third Party Corporate Information that is in the care, custody or control of the Insured Organization, or a third party for whom the Insured Organization is legally liable

Evaluation of the Data Breach

- Forensic Investigation and Legal Review

Managing the Short-Term Crisis

- Notification and Credit Monitoring
- Public Relations

Handling the Long-Term Consequences

- Class-Action Lawsuits
- Regulatory Fines, Penalties, and Consumer Redress
- Reputational Damage
- Income Loss
**Cyber Insurance Considerations**

- Assess your company’s unique cyber risk profile
- Examine your current coverage in light of your company’s risk
- Ensure that cyber coverage is adequate to address those risks
- If your company entrusts data to vendors, ensure that the cyber policy provides coverage for vendor incidents
- Consider insurance requirements for vendors
MEANWHILE...ACROSS THE POND
Best Practices & Most Important Learnings

“Training, Training, Training.”

“External Assessment every 6 to 12 months.”

“Conduct a deep-dive analysis into your information governance practices (what you have, do we need it, where is it, who accesses it, how is it stored).”

“Communication between legal and IT regarding vendors.”

“Review cyber insurance policy to know what it covers.”

“Test vendors rigorously and regularly.”

“Security department presents at every quarterly board meeting.”
REBECCA PERRY, CIPP/US/G
Director of Professional Services
Jordan Lawrence
rperry@jordanlawrence.com

JEFF C. DODD
Partner
Andrews Kurth LLP
jeffdodd@andrewskurth.com

JIM ELLIOTT
Assistant Regional Director,
Southwest Region
Federal Trade Commission
JELLIOTT@ftc.gov

MATTHEW G. NIELSEN
Partner
Andrews Kurth LLP
matthewnielsen@andrewskurth.com