EFFECTIVE INCIDENT RESPONSE

PRESENTED TO
NAAG/NASCO

October 17, 2016 - Washington, DC

Paul H. Luehr – Exec. Managing Director, Stroz Friedberg
# Understanding Risk: Data Breach Costs

<table>
<thead>
<tr>
<th>Indirect Costs:</th>
<th>Direct Costs:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staff hours</td>
<td>Outside Counsel</td>
</tr>
<tr>
<td>Lost Goodwill</td>
<td>Outside Experts</td>
</tr>
<tr>
<td>Customer “Churn”</td>
<td>ID Theft Insurance</td>
</tr>
<tr>
<td></td>
<td>Notification Costs</td>
</tr>
</tbody>
</table>

- **66%** Indirect Costs
- **34%** Direct Costs

Source: 2016 Cost of Data Breach Study: Global Analysis, Sponsored by IBM, Conducted by Ponemon Institute LLC (June 2016)
Global Data Breach Cost – Per Capita, by Industry

Source: Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis,” Sponsored by IBM (June 2016)
Healthcare Example:
HIPAA Data Breach Notification Rule,
45 CFR §§ 164.400-414

Trigger: impermissible “use, acquisition, access, use, or disclosure” of “protected health information” (PHI) that is not “secure” (i.e. encrypted/destroyed)

Unless there’s a “low probability” that PHI as been compromised, considering:
(i) The nature and extent of PHI and the likelihood of re-identification;
(ii) The unauthorized person who used or received the PHI;
(iii) Whether the PHI was actually acquired or viewed; and
(iv) The extent to which the risk to the PHI has been mitigated.
Varied Notification Timelines:

- Business: Often 24 hours by contract
- State Agency: Varies, CT DOI e.g. – 5 days
- Victims: Florida (e.g.) - 30 +15 days
  Others: “without unreasonable delay”
- HHS: Victims within 60 days, HHS and media if over 500 victims
- EU: 72 hours to notify “proper channels” (in 2018 under GDPR)
Three Critical Areas of Operations

- Performing Regular Risk Assessments
- Developing a Robust Incident Response (IR) Plan
- Creating an Effective Governance Structure
Prevention: Security Assessments

The Assessment Process:

- Business priorities, constraints
- Operational environment

Security Standard:
- NIST, ISO 27001, CSC(SANS 20), HIPAA, etc.

Prioritized security risk findings & recommendations
Prevention: A Robust IR Plan

- Management endorsement
- Cross-disciplinary team
- Contact lists
- Legal analysis and timeline
- Categories of adverse events
- Escalation process
- Communications plan
An Effective Team

- Multiple representatives
- Led by counsel
- With contact sheet for:
  - Outside counsel
  - Forensic experts
  - Crisis communicators
  - Notification firms
  - Insurance agent/broker
  - Law enforcement
Prevention: Timing Expectations

**Average Time to Contain = 59 to 82 days**

Source: Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis” Sponsored by IBM (June 2016)

Forensic Investigation Timeline

- **Preservation** (4 – 14 days)
- **Rebuild Drives**
- **Forensic Analysis** (21 – 28 days)
- **Malware Analysis** (10 – 21 days)
- **Scanning** (21 – 28 days)
- **Report** (10 – 21 days)

Average Time to Contain = 59 to 82 days

Source: Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis” Sponsored by IBM (June 2016)
Prevention: Sound Governance

- Roles and Responsibilities
- Policies & Procedures
- Privacy by Design
- Security by Example
Questions?