David Phillips, Managing Director
Berkeley Research Group
www.ThinkBRG.com
dphillips@ThinkBRG.com

Preparing for the Big One

Advancing the Culture of Security
An ever-more connected world . . .

**People**
- Wellness monitoring
- Medical case management
- Social needs

**Communities**
- Traffic status
- Pollution alerts
- Infrastructure checks

**Goods & Services**
- Track materials
- Speed distribution
- Product feedback

**Environment**
- Pollution checks
- Resource status
- Water monitoring

**Homes**
- Utilities control
- Security monitoring
- Structure integrity
With more devices interacting. . .

2010 Devices surpassed people by almost 2:1
Forecasts expect >6:1 ratio by 2020

<table>
<thead>
<tr>
<th></th>
<th>2003</th>
<th>2010</th>
<th>2015</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>World Population</td>
<td>6.3 Billion</td>
<td>6.8 Billion</td>
<td>7.2 Billion</td>
<td>7.6 Billion</td>
</tr>
<tr>
<td>Connected Devices</td>
<td>500 Million</td>
<td>12.5 Billion</td>
<td>25 Billion</td>
<td>50 Billion</td>
</tr>
<tr>
<td>Connected Devices per Person</td>
<td>0.08</td>
<td>1.84</td>
<td>3.47</td>
<td>6.58</td>
</tr>
</tbody>
</table>
What data is at Risk?

All Digital Assets

- Business plans, (e.g., bids, acquisition strategies)
- Trading algorithms
- Contracts (e.g., with customers, suppliers, distributors)
- Employee log-in credentials
- Company facilities security information
- Proprietary product designs
- Confidential source code
- Employee, customer, contractor and supplier lists
- Client data
- PII, PHI, PCI data
Self Governance in the Rear View Mirror

• White House has issued 3 Executive Orders in two years
  – Blocking property for malicious cyber activities, April 2015
  – Promoting cybersecurity information sharing, February 2015
  – Improving critical infrastructure cybersecurity (EO 13636), February 2013

• Securities and Exchange Commission posts guidelines for cyber security disclosure and calls out the Board of Directors role in oversight of cyber risk

• FCC has jurisdiction to fine companies for substandard information security protections

• ABA Resolution / NACD Recommends New Committee

• Standard and Poor’s cybersecurity baseline can effect company ratings
“Of even greater concern is the fact that corporate boardrooms seem determined to adopt ostrich-like behavior and ignore the problem.”
“RESOLVED, that the American Bar Association encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected.”
“Ensuring the adequacy of a company’s cybersecurity measures needs to be a critical part of a board of director’s risk oversight responsibilities.”

Luis A. Aguilar
U.S. Securities and Exchange Commissioner
Target Corporation lost the motion to deny Class certification for the data breach in 2013. This will allow financial institutions to suit to recoup expenses for reissuing cards and reimburse fraud losses.

The claims against Target are ... being negligent in preventing hackers from accessing customer data.
Executive Cybersecurity Strategy

Cybersecurity Program Template

- **Risk Management**
  - Risk Heat Map
  - Crisis Planning
  - Cyber Budget Priorities
  - Business Continuity / Resilience

- **Information Governance**
  - Comms Planning / Public Relations
  - Regulatory Framework
  - Privacy/Record Management

- **Incident Response**
  - Prepare
  - Detect
  - Respond
  - Transform

- **Security Awareness**
  - Cultural Assessment
  - Policy Compliance
  - IT Security Metrics
  - Awareness Campaign

- **Essential Protection**
  - Security Ops
  - Vulnerability Management
  - Architecture Design
  - Technology Solutions

Security Culture
People, Process, and Technology

Technology

Process

People

Technology

People

Process
1. Designate new board committee for Data and Technology, similar to Compensation or Risk
2. Recruit new directors for the committee who understand the IT and Security landscape
3. Seek Board and CxO level cybersecurity advisors
4. Require regular Board updates on cybersecurity metrics and program progress
5. Assess / exercise current risk management program for cybersecurity gaps
6. Approve updated cybersecurity metrics and goals
7. Review / approve information governance roadmap including budget requirements
8. Direct counsel to review cyber insurance coverage
9. Establish review process for third party vendors
Board of Directors Overall Must

- Be knowledgeable of their responsibility.
- Take action to reduce the company’s security exposure
- Demonstrate the company has a new program
- Validate the program is following reasonable industry best practices.
- Demonstrate the company culture is following the new program
## Sample Board Questions

<table>
<thead>
<tr>
<th>Before an Incident</th>
<th>After an Incident</th>
</tr>
</thead>
<tbody>
<tr>
<td>Which Board committee leads Incident Response risk?</td>
<td>What appears to have been copied / stolen? Do we know the value of what was taken? Other financial impacts?</td>
</tr>
<tr>
<td>Which department head leads IR the incident investigations?</td>
<td>Who discovered the breach, internally or outside law enforcement?</td>
</tr>
<tr>
<td>What is our financial exposure to a major breach?</td>
<td>What is the material impact to operations?</td>
</tr>
<tr>
<td>How much cash reserves have we put aside for an event?</td>
<td>How does this incident adjust our security strategy?</td>
</tr>
<tr>
<td>How many incidents do we have compared to same period last year?</td>
<td>What is our responsibility to disclose/notify?</td>
</tr>
<tr>
<td>Do we have deep the right relationships and retainers in place?</td>
<td>Which stage of our IR Plan are we in now? Is the incident ongoing?</td>
</tr>
</tbody>
</table>
The 90-Day Action Plan

- Exercise incident response / crisis management plan
- Reconcile overlapping regulatory reporting obligations to an agreed company framework
- Assess exposure from electronic records management, privacy, and data classification
- Establish security metrics and culture program to include robust education and awareness training
- Update risk management plan to include proper budget, insurance coverage, record retention, organizational accountability
• Corporate liability coverage is not enough
  – All insurers are excluding electronic data loss and privacy breach from the liability policy
  – A separate policy for data breach is required
• Cyber policies are a long way from coverage the comprehensive damage
  – Limitations and common exclusions may be surprising. See the follow two slides
  – Negotiate the exclusion language to press your position
• Have an insurance strategy for a catastrophic event.
  – If the limits of the policy (once you get past the exclusions) is $5M, layer multiple policies to get to the $ amount of coverage your risk model indicated for annualized loss expectancy (ALE).
• CFO needs to have cash reserves to cover the remainder which may impact quarterly reporting
  – which is why the financial team needs to be in the planning process
<table>
<thead>
<tr>
<th></th>
<th>Common Cybersecurity Insurance Exclusions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bodily Injury or Damage. These are covered under the general liability policy.</td>
</tr>
<tr>
<td>2</td>
<td>Loss of paper files, as they are not electronic.</td>
</tr>
<tr>
<td>3</td>
<td>War, Invasion, &amp; Terrorism</td>
</tr>
<tr>
<td>4</td>
<td>Patent and Copy Right infringement. These are normally included in an intellectual property cover policy.</td>
</tr>
<tr>
<td>5</td>
<td>Mechanical and electrical breakdown / failure. No kinetic damage.</td>
</tr>
<tr>
<td>6</td>
<td>Failure to following basic security best practices.</td>
</tr>
<tr>
<td>7</td>
<td>Losses from portable electronic devices, i.e. laptops.</td>
</tr>
<tr>
<td>8</td>
<td>Unencrypted data</td>
</tr>
<tr>
<td>9</td>
<td>Data entrusted to third-parties. Third-parties need to have the insurance coverage.</td>
</tr>
<tr>
<td>10</td>
<td>Claims/fines brought by government or regulators</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity Insurance Best Practices</td>
</tr>
<tr>
<td>---</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>1</td>
<td>Work with a knowledgeable insurance broker.</td>
</tr>
<tr>
<td>2</td>
<td>Read the policy terms with your legal counsel and head of IT</td>
</tr>
<tr>
<td>3</td>
<td>Model the worst case scenario for negative financial impact and purchase a policy limit (and sub-limit) that fits.</td>
</tr>
<tr>
<td>4</td>
<td>Shop for an insurer who will take your technical controls and security policies into account when setting premiums.</td>
</tr>
<tr>
<td>5</td>
<td>Examine the insurance carrier’s rating, higher ratings indicate a stronger company</td>
</tr>
<tr>
<td>6</td>
<td>Consider retroactive coverage as some policies only include from policy origination date.</td>
</tr>
<tr>
<td>7</td>
<td>Be aware of panel provisions that require your outside counsel, consultant, or investigator to be on a preapproved list kept by the insurance carrier.</td>
</tr>
</tbody>
</table>
Data and Culture

- FAA Near Miss Data Base is a voluntary reporting structure.
- Does a high number of reported incidents indicate a dangerously run operation?
- Or is it an indicator of a culture of reporting?
People are the Center of Security

- Technology alone is not working
- People design, configure, and run the technology
- Technology enforces a human policy, a behavioral policy
- People decide to bypass technology
Understanding People’s Beliefs – Culture

- How do people decide which rules to follow?
- Humans determine
  - Acceptable risk
  - If security events make an incident
  - Degree of response
- Culture can seem “soft”, difficult to grasp
  - Qualitative data (ex. Interview) is solid
  - Results are evidence

“Advancing the Culture of Security”
Cultural Differences, Competing Priorities

“The way we do things around here …”

“Is it a bottom line issue …”

“We sell clothes …”

“This better not take long …”
Culture Trumps Strategy (& technology)

• Superior cultures dramatically out performs the competition
  - 1996 Olympic Training Case
  - PayPal Startup Vision
  - Apple Transformative Culture

• Studying Organizational Culture is not New

• High Reliability is Our Goal
  - The right process and models get us there
Measuring Cultural Differences

- Measurable when handled with the right processes and tools
- Competing Security Cultures Framework (CSCF)
- Collecting organizational artifacts (Qual & Quan) allows a plot of today’s culture
- FORCE behavioral changes
Cultural Transformation FORCE

- 5 core behavior values drive the characteristics of a Highly Reliable Security Program
- Measure these, shape new behaviors, and set new goals
- Change a culture and you change a habit...actions done without having to think about it.
Applying FORCE

Composite FORCE scorecard compares behaviors over time and between organizations.

Measuring the shape of your security culture.
Cultural Capabilities Maturity Model shows progress from adhoc (1) to an organization in control (5) of security culture.

At Mastery (5), the org is continually transforming the current security cultural state.
Transformation as Cultural Maturity

5 - Mastery
4 - Transformation
3 - Visibility
2 - Awareness
1 - Instinct

Security Culture Transformation Program
Security FORCE Project
Security Culture Diagnostic Project

Start
3 months, 6 months, 9 months, 12 months
Measuring Cultural Maturity

- HRSP targets can yield monetary measurements
- Culture Capabilities Maturity Model demonstrated by applying risk modeling
- Fact: Weak organizations cost the company money

![Annual Security Incident Losses](chart)

<table>
<thead>
<tr>
<th>Culture Type</th>
<th>Annual Security Incident Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak Culture</td>
<td>$350,000</td>
</tr>
<tr>
<td>Moderate Culture</td>
<td>$204,000</td>
</tr>
<tr>
<td>Strong Culture</td>
<td>$88,000</td>
</tr>
</tbody>
</table>
Next Steps to Becoming an HRSP

Advancing the Culture of Security

1. Learn about security culture and think like People-Centric Security
2. Use CSCF and FORCE model to assess your organizations current state
3. Set yearly goals for your future culture state
4. Launch FORCE transformation program to measure and migration to Cultural Maturity
Get Prepared, Stay Prepared
Thank You!

Additional Resources

- dphillips@ThinkBRG.com
- http://lancehayden.net
- http://securityispeople.com
Security is People!