CYBERSECURITY

Top 10 Cost Effective Strategies for Risk Reduction
GOALS FOR THIS SESSION

- Scare the heck out of you!
- Define cybersecurity
- Share Our Top 10 Cost Effective Strategies List
“There are only two types of companies: those that have been hacked, & those that will be. Even that is merging into one category: those that have been hacked & will be again.”

Robert Mueller, FBI Director
On Cyber Threat Landscape
CYBERSECURITY STATISTICS (GLOBAL)

• 781 – number of reported breaches in 2015
• $400M – est. total annual cost of attacks
• $2.1Trillion – projected for 2019
• $3.8M – average total cost breaches
• $6.5M – average total cost breaches in US

Source: DMR Stats
CYBERSECURITY STATISTICS (GLOBAL)

- 23% - increase in breaches from 2013-2015
- 80-90M – annual cybersecurity incidents
- 38% - increase in incidents 2014-2015
- Phishing and malware – top means of cyber attack in 2015
- 12% - percentage of people that opened a phishing message in 2016 and clicked on the malicious attachment or link

Source: DMR Stats
**CYBERSECURITY STATISTICS (GLOBAL)**

- Most attached industry in 2015
  - Healthcare!

*Source: DMR Stats*
HEALTHCARE BREACHES

• Data breaches in Healthcare totaled 112 million records in 2015*
• Cost per record $154**
• According to the OCR, 253 healthcare breaches, affected 500 individuals for combined 112 million records*
  ▪ 38% were reported as Unauthorized Access/Disclosure
  ▪ 21% were Hacking/IT Incident breaches
    • 90% of the top ten entity breaches were reported as a Hacking/IT Incident
  ▪ 29% of all breaches were theft
  ▪ 12% who knows?

**Source:  DMR Stats February 4, 2016
<table>
<thead>
<tr>
<th>Organization</th>
<th>Records Breached</th>
<th>Type of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Anthem</strong></td>
<td>78,800,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Premera</strong></td>
<td>11,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Excellus</strong></td>
<td>10,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>UCLA Health</strong></td>
<td>4,500,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>mie</strong></td>
<td>3,900,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>CareFirst</strong></td>
<td>1,100,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>DMAS</strong></td>
<td>697,586</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Georgia Department of Community Health</strong></td>
<td>557,779</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>Beacon Health System</strong></td>
<td>306,789</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td><strong>DJO Global</strong></td>
<td>160,000</td>
<td>Laptop Theft</td>
</tr>
</tbody>
</table>

**2015 Total**: 111,022,154 (almost 35% U.S. population)
HEALTHCARE BREACHES

• Predict big breaches will make the headlines, but the small ones cost the most money
• 91% of all Healthcare organizations reported at least one breach in the past 2 years
• Medical records are worth up to 10 times more than credit card numbers on the black market
• Most breaches due to employees mishandling or losing information “unauthorized access/disclosure”

Source: 2016 Experian Data Breach Industry Forecast
In recent security discussions, there are references to both “cybersecurity” & “information security.” The terms are often used interchangeably, but in reality, *cybersecurity is a part of information security.*
DEFINING CYBERSECURITY

• **Information security** deals with protecting information, regardless of its format: physical documents, digital, intellectual property in people’s minds & verbal or visual communications

• **Cybersecurity** is concerned with protecting digital assets — everything from networks to hardware & information processed, stored or transported by internetworked information systems
Objective of cybersecurity is threefold, involving the critical components of confidentiality, integrity & availability.
DEFINING CYBERSECURITY

NIST definition:
• The process of managing cyber threats & vulnerabilities & for protecting information & information systems by
  ▪ identifying,
  ▪ defending against,
  ▪ responding to
  ▪ & recovering from attacks
## NIST Framework Overview

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness &amp; Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes &amp; Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies &amp; Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
</tbody>
</table>

*Note: BKD National Health Care Group*
TOP 10

Cost-effective strategies for risk reduction
#1 – KNOW WHERE YOUR DATA IS STORED

Document and maintain accurate information asset inventories, including all relevant assets that store or transmit sensitive data

• Data flow analysis
• Consolidate all valuable data into most singular storage possible
#2 – TAKE ADVANTAGE OF SECURITY CONTROLS

Establish, implement and actively manage security configuration settings for all hardware and software for servers, workstations, laptops, mobile devices, firewalls, routers, etc.

- System/device hardening
- Strong password security
- Limit administrative privileges
- Grant only the minimum required access to perform job functions
#3 – KNOW WHO CAN ACCESS YOUR DATA

Align logical and physical access authorization, establishment, modification & termination procedures applicable to networks, operating systems, applications & databases

• Screen employees prior to employment
• Document additions and modifications
• Timely removal of terminated employees
• Limit vendor remote access
#4 – IMPLEMENT DATA LOSS PREVENTION CONTROLS

Organizations must limit access to removable media, CDs, portable drives, email & file transfer websites

- Leverage existing policies
- Write clear policies that encompasses device use & disposal of information
- Wipe devices no longer in use & then physically destroyed
#5 – ENSURE ALL CRITICAL DATA IS ENCRYPTED

Adoption of data encryption, for data in use, in transit and at rest, provides mitigation against data compromise

• Encrypt all hard drives on all portable devices
• Protect backup information
#6 – EFFECTIVE PATCH MANAGEMENT

Ensure all systems, regardless of function or impact, have recent operating systems, application patches applied and any business-critical applications are maintained at the most current feasible level for your organization

- Evaluate & test critical patches in timely manner
- Apply patches for riskiest vulnerabilities first
- Third-party applications (Java, Adobe, Flash, etc.) must also be managed
#7 – PERFORM RISK ASSESSMENTS

Perform an information security risk assessment that is flexible and responds to changes in your environment. Specific focus should be on all protected information & protected health information.
#8 – EDUCATE PERSONNEL & HOLD THEM ACCOUNTABLE

Provide staff training on security best practices, internal policies & new threats. Focus on social engineering, phishing & physical security concerns.

- Educate all personnel at least annually
- Make sure new hire onboarding process includes this topic
- Accountability includes ALL personnel — especially senior management — who must lead by example
Conduct vulnerability scans and penetration tests to identify and evaluate security vulnerabilities in your environment

- Security controls provide most value when they are audited & monitored for compliance &/or maintenance
- Annual audits provide necessary insights into keeping security controls optimized & properly fitted to environments employed to protect
Management's ultimate goal should be to minimize damage to the institution and its customers through containment of the incident and proper restoration of information systems

- Conduct analysis of past incidents
- Use an incident response team
- Determine who will be responsible
Resources

NIST  www.nist.gov/cyberframework
   NIST Framework
Homeland Security  www.dhs.gov/topic/cybersecurity
Krebs On Security  www.krebsonsecurity.com
   Security Newsletter
SANS  www.sans.org
   SysAdmin, Audit, Networking, and Security
Security Tools  www.sectools.org
   Open source security tools, be careful and use at your own risk
Upcoming BKD Webinar

October 19, 2016
11:30-12:30 central time
Insurance Coverage for Cybersecurity Threats

QUESTIONS?
THANK YOU!

FOR MORE INFORMATION

Cindy Boyle, CPA, CIA, CITP, CISA
Partner – IT Risk Services Leader
cboyle@bkd.com
501-372-1040
BKD THOUGHTWARE®
Sign up at bkd.com/subscribe

articles // emails // presentations // videos // webinars