National Cyber Security Awareness Month

Week Two: Creating a Culture of Cybersecurity at Work
Webinar Recording and Evaluation Survey

• This webinar is being recorded and will be made available online to view later
  o Recording will also be available at www.naco.org/webinars

• After the webinar, you will receive a notice asking you to complete a webinar evaluation survey. Thank you in advance for completing the webinar evaluation survey. Your feedback is important to us.
Tips for viewing this webinar:

- The questions box and buttons are on the right side of the webinar window.
- This box can collapse so that you can better view the presentation. To unhide the box, click the arrows on the top left corner of the panel.
- If you are having technical difficulties, please send us a message via the questions box on your right. Our organizer will reply to you privately and help resolve the issue.
Today’s Speakers

Mr. Ralph Johnson
Chief Information Security and Privacy Officer
King County, Wash.

Mr. Peter Romness
Cybersecurity Business Development Manager
Cisco Systems, Inc.

Ben Scribner
Cyber Education and Awareness,
U.S. Department of Homeland Security
Creating a Culture of CyberSecurity at Work
Ralph Johnson, CISSP, HISP, CISM, CIPP/US

Chief Information Security and Privacy Officer –
King County Washington
Adjunct Instructor ITT Technical Institute, Seattle
Past Governance Board President – Holistic Information
Security Practitioner Institute (HISPI)
Member – MS-ISAC Executive Committee
Member – MS-ISAC Trusted Purchasing Alliance Product Review Board
Member – MS-ISAC Education and Awareness Committee
National Association of Counties (NACo) Cyber-Security Task Force
Hashtag #CyberAware in your social media messages.
Why do we need a culture of cybersecurity

As high-profile cybersecurity incidents reveal the true impact a data breach can have on an organization businesses are recognizing the need for new approaches to information security.

In an era of increasing data breaches organizations must actively make cybersecurity a part of their culture and equip every employee with the knowledge and tools to prevent and address data security issues.
4537 breaches made public consisting of over 827.4M records breached since 2005

http://www.privacyrights.org/

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Breaches</th>
<th>Records</th>
<th>Average Records / Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>2005</td>
<td>136</td>
<td>52,821,610</td>
<td>388,394.19</td>
</tr>
<tr>
<td>2006</td>
<td>482</td>
<td>48,607,177</td>
<td>100,844.76</td>
</tr>
<tr>
<td>2008</td>
<td>354</td>
<td>49,659,455</td>
<td>140,280.94</td>
</tr>
<tr>
<td>2009</td>
<td>251</td>
<td>218,893,415</td>
<td>872,085.31</td>
</tr>
<tr>
<td>2010</td>
<td>604</td>
<td>12,341,662</td>
<td>20,433.21</td>
</tr>
<tr>
<td>2011</td>
<td>598</td>
<td>66,133,574</td>
<td>110,591.26</td>
</tr>
<tr>
<td>2012</td>
<td>680</td>
<td>27,988,987</td>
<td>41,160.27</td>
</tr>
<tr>
<td>2013</td>
<td>622</td>
<td>257,840,933</td>
<td>414,535.26</td>
</tr>
<tr>
<td>2014</td>
<td>296</td>
<td>67,876,246</td>
<td>229,311.64</td>
</tr>
<tr>
<td>2015</td>
<td>116</td>
<td>132,245,967</td>
<td>1,140,015.44</td>
</tr>
</tbody>
</table>
Costs associated with breaches are rising. According to Ponemon Institute and IBM the average total cost of a data breach for the participating companies increased 23% since 2013.
Tips for creating a culture of cybersecurity

- Assess risks and assets
- Update data security plans regularly
- Implement policies, procedures and best practices for data security
- Enforce policies
- Lead by example
- Extend cybersecurity awareness outside the office
- Educate and train employees
- Diversify and repeat
- Empower employees
- Assess training and awareness programs
Assess risks and assets

Begin with an assessment of cybersecurity risks and assets

- Know the risks facing the organization
- Maintain an up-to-date inventory of the organization's information assets
Perform assessments on a regularly
Stay up-to-date with new or evolving threats and/or address new business functions that may increase existing risks, or create new ones.
Implement policies, procedures and best practices for data security

Policies should address issues such as;

- Acceptable use
- E-mail
- Passwords
- Social media
- Incident reporting
- Backup and recovery
- Software installation and licensing
- Disaster recovery

Based on best practices, industry standards and regulatory guidance.

Easily accessible to all employees and should not be so restrictive or onerous that they discourage compliance.
Enforce policies

- Highlight data security as an employees' responsibility
- Impose consequences for non-compliance to make employees see data security as part of their job responsibility.
Employees are more likely to take cybersecurity measures seriously when executives and managers confirm the organization's commitment to information security by actively participating in cybersecurity programs, training and other measures.
Extend cybersecurity awareness outside the office

Employees are more likely to pay attention when organizations stress the importance of data protection in their personal family life, as well as in the workplace.
Employees are reluctant to follow policies they don’t understand.

- Educate employees on the reasons behind policies.
- Training should be mandatory and carried out on a regular basis.
Convey the importance of cybersecurity by using a variety of resources:
- Posters
- Newsletters
- Email tips
- Blogs
- Reminders
- Staff meetings
Encourage employees to provide suggestions and feedback to invest employees in data protection and help gauge the effectiveness of the organization's data security efforts.
Assess training and awareness programs

- Regularly assess security awareness programs and related training to ensure they address all relevant issues, identify knowledge gaps and are achieving the organization's goals.

- Mock exercises, exams or interviews can verify that employees understand the training materials, while surveys or other resources can help evaluate the program's efficiency or identify areas for improvement.
Information security is an organization issue

Information Security Is the Responsibility of Everyone
Ralph Johnson, CISSP, CISM, HISP, CIPP/US
King County
Chief Information Security and Privacy Officer
ralph.johnson@kingcounty.gov
206-263-7891 (Office)
206-818-7929 (Mobile)
Creating a Culture of Cybersecurity at Work

Peter Romness
promness@cisco.com
Cybersecurity Solutions Lead
US Public Sector

October 2015
Send phishing emails to just 10 employees will get hackers inside corporate gates 90 percent of the time.

Verizon 2015 Data Breach Investigations Report (DBIR)

Attackers use phishing techniques because they work and because the less-sophisticated approach drew less scrutiny from defenders.

Symantec 2015 Internet Security Threat Report
Technology Doesn’t Cover Everything

People  Process  Technology
# Technology Doesn’t Cover Everything

## Example: NIST Framework

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

- **Only half of the Framework’s Categories are addressed by technology**
- **Highlights the importance of both people and process in cybersecurity**
Buy-in from the whole team

Highlight the benefits to all:

- Personal protection - privacy and safety
  At work and at home
- Organization reputation
- Preserve the trust of those we serve
- Save money and jobs

Reward positive actions and results

- Highlight the positive
Effective Workplace Training

Should be:

✓ Brief and Engaging
✓ Frequent
✓ Achievable – even easy
✓ Persistent
✓ Consistent
✓ Fun!
Thank You
Who needs to practice good cybersecurity?

Consider cyber when…
- Protecting private information
- Connecting with care and being web wise
- Being a good online steward

Consider cyber in…
- Acquisitions
- Policies
- Risk assessments
- etc.

Actively…
- Identify
- Protect
- Detect
- Respond
- Recover
Join us this NCSAM by educating and empowering your community to take steps to protect themselves and their families online:

- **Promote** NCSAM in your organization or community
- **Become** a NCSAM Champion
- **Participate** in NCSAM 2015 Twitter chats
- **Attend** a NCSAM event in your area
- **Use** the NCSAM hashtag – #CyberAware – to promote your organization’s involvement in raising cybersecurity awareness

Learn more at:

- dhs.gov/national-cyber-security-awareness-month
- StaySafeOnline.org/ncsam
niccs.us-cert.gov

• Training/Education Catalog
• Workforce Development toolkit
• Workforce Framework

Questions? contact: NICCS@hq.dhs.gov
Q&A

You may ask a question using the questions box on the right side of the webinar window.
Contact Information

Jerryl Guy, MS, MCSE, CISSP
IT Manager, NACo
Email: jguy@naco.org
Phone: (202) 942-4229