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
    - 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
Cycbersecurity Business Developme
Manager
Cisco Systems, Inc.

Ben Scribner
Cyber Education and
Awareness,
U.S. Department of Homeland
Security

Creating a Culture of CyberSecurity at Work

National Association of Counties (NACo)
National Cyber Security Awareness Month Webinar
October 7, 2015

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

King County
Information
TECHNOLOGY

National Cyber Security Awareness Month

Our Shared Responsibility
staysafeonline.org
National Cyber Security Awareness Month

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.

Information breaches

4537 breaches made public consisting of over 827.4M records breached since 2005

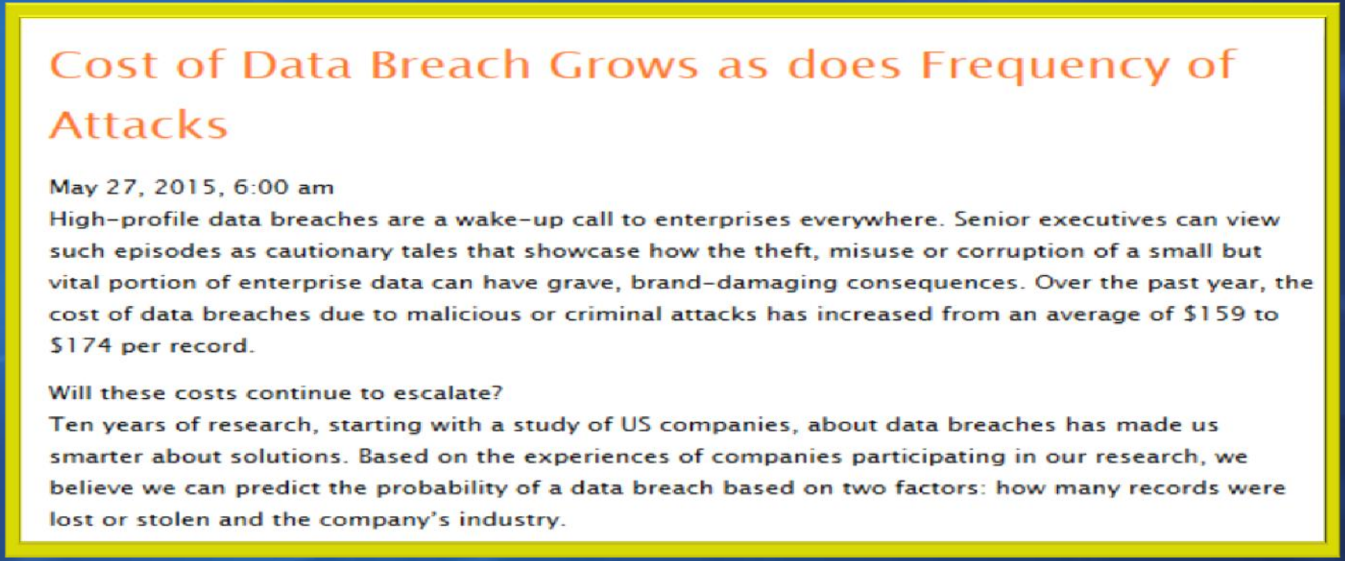
http://www.privacyrights.org/

Year	Number of Breaches	Records	Average Records / Breach
2005	136	52,821,610	388,394.19
2006	482	48,607,177	100,844.76
2007	451	129,965,681	288,172.24
2008	354	49,659,455	140,280.94
2009	251	218,893,415	872,085.31
2010	604	12,341,662	20,433.21
2011	598	66,133,574	110,591.26
2012	680	27,988,987	41,160.27
2013	622	257,840,933	414,535.26
2014	296	67,876,246	229,311.64
2015	116	132,245,967	1,140,015.44

2015 – as of September 2015

Breach costs

- Costs associated with breaches are rising.
  - According to Ponomon Institute and IBM the average total cost of a data breach for the participating companies increased 23% since 2013.



Cost of Data Breach Grows as does Frequency of Attacks

May 27, 2015, 6:00 am

High-profile data breaches are a wake-up call to enterprises everywhere. Senior executives can view such episodes as cautionary tales that showcase how the theft, misuse or corruption of a small but vital portion of enterprise data can have grave, brand-damaging consequences. Over the past year, the cost of data breaches due to malicious or criminal attacks has increased from an average of $159 to $174 per record.

Will these costs continue to escalate?

Ten years of research, starting with a study of US companies, about data breaches has made us smarter about solutions. Based on the experiences of companies participating in our research, we believe we can predict the probability of a data breach based on two factors: how many records were lost or stolen and the company's industry.

Tips for creating a culture of cybersecurity

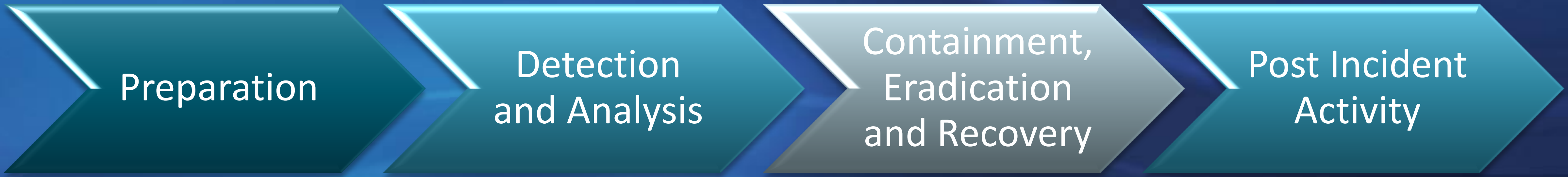
- Assess risks and assets
- Update data security plans regularly
- Implement policies, procedures and best practices for data security
- Enforce policies
- Lead by example
- Extend cybersecurity awareness outside the office
- Educate and train employees
- Diversify and repeat
- Empower employees
- Assess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

Update data security plans regularly

- 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.



Preparation

Detection and Analysis

Containment, Eradication and Recovery

Post Incident Activity

Implement policies, procedures and best practices for data security

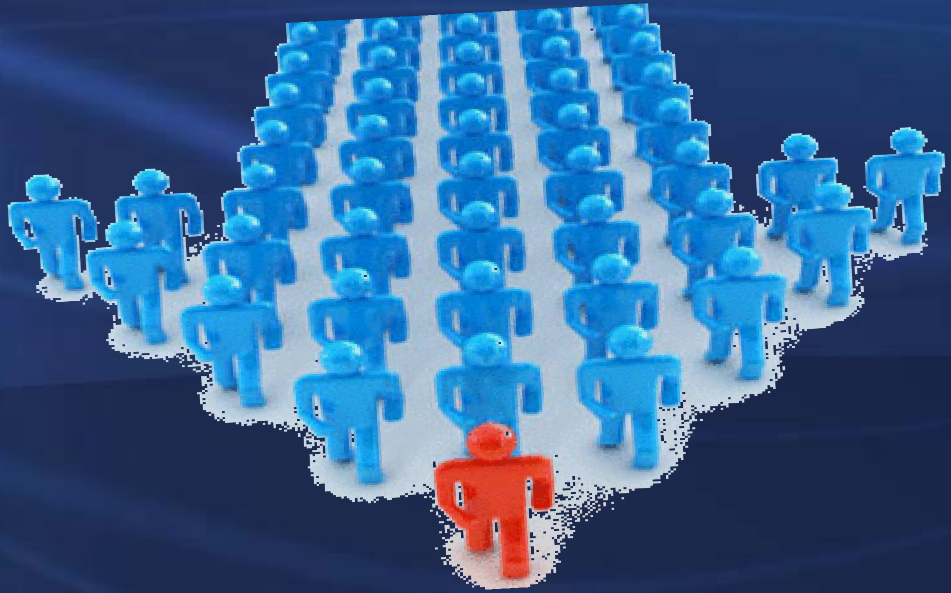
- Policies should address issues such as;
  - Acceptable use
  - E-mail
  - Passwords
  - Social media
  - Incident reporting
  - Backup and recovery
  - Software installation and licensing
  - Disaster recovery
- Based on best practices, industry standards and regulatory guidance.
- Easily accessible 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 their job responsibility.

Lead by example

- 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.

Educate and train employees

- 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.

Diversify and repeat

- Convey the importance of cybersecurity by using a variety of resources;
  - Posters
  - Newsletters
  - Email tips
  - Blogs
  - Reminders
  - Staff meetings

Empower employees

- 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**

Contact information

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)

King County
Information
TECHNOLOGY

Creating a Culture of Cybersecurity at Work

Peter Romness
promness@cisco.com

Cybersecurity Solutions Lead
US Public Sector

October 2015

© 2013 Cisco and/or its affiliates. All rights reserved.

Think Like an Attacker

Sending phishing emails to just 10 employees will get hackers inside corporate gates 90 percent of the time

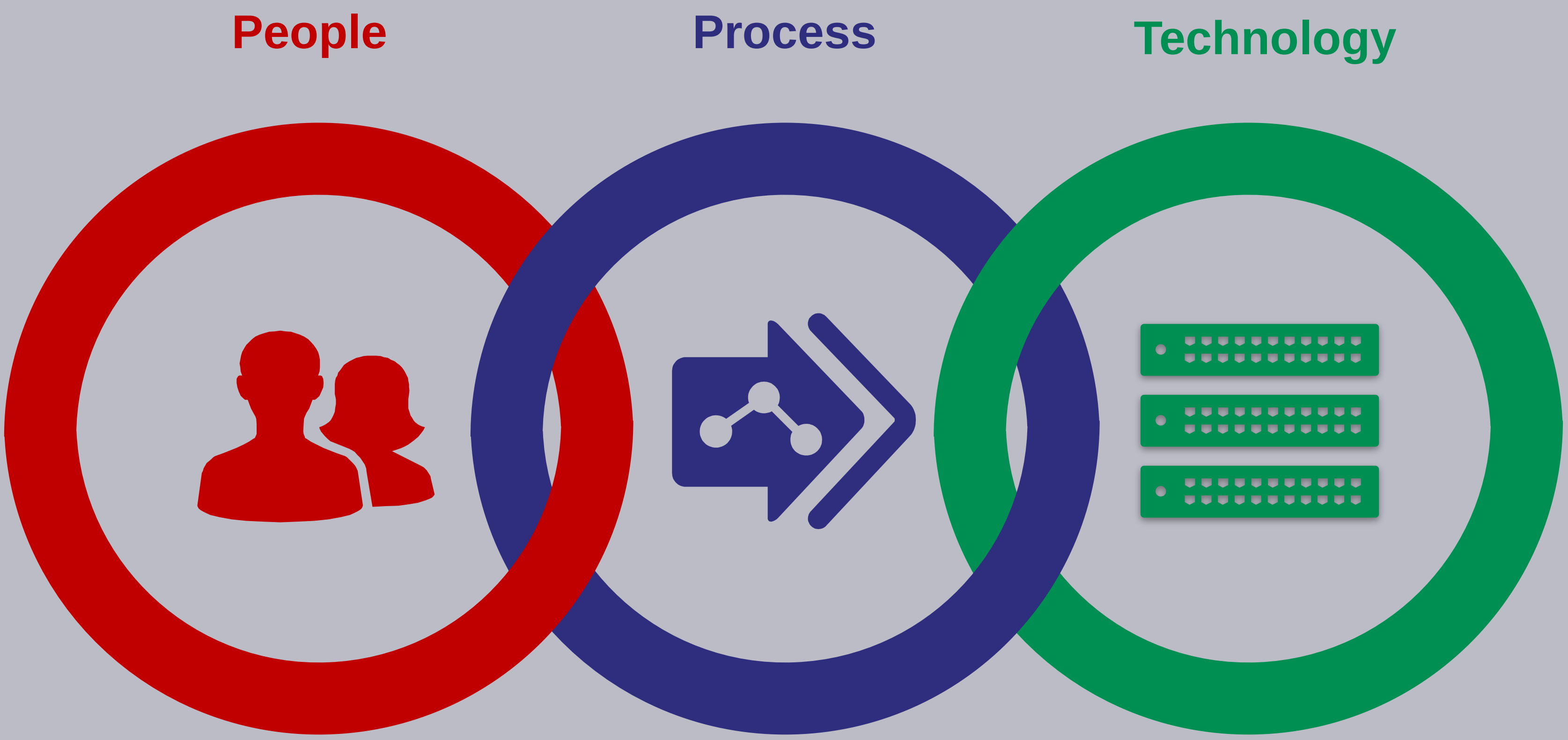
Verizon 2015 Data Breach Investigations Report (DBIR)

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

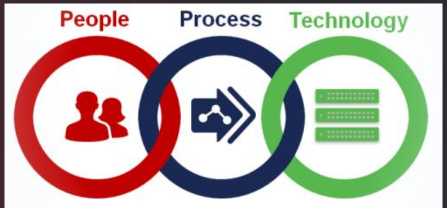
Symantec 2015 Internet Security Threat Report

© 2015 Cisco and/or its affiliates. All rights reserved.

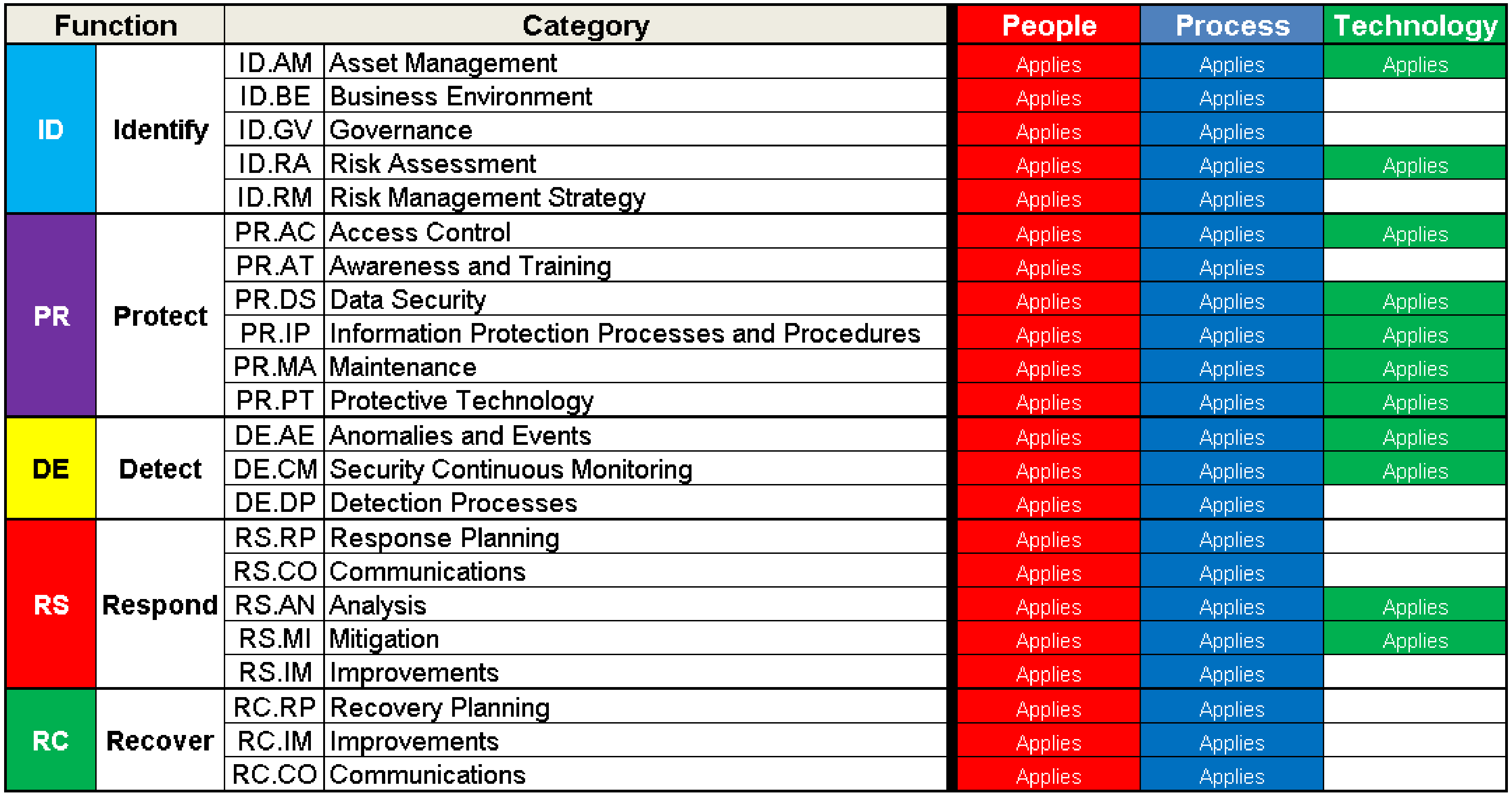
Technology Doesn’t Cover Everything



Technology Doesn’t Cover Everything



Example: NIST Framework

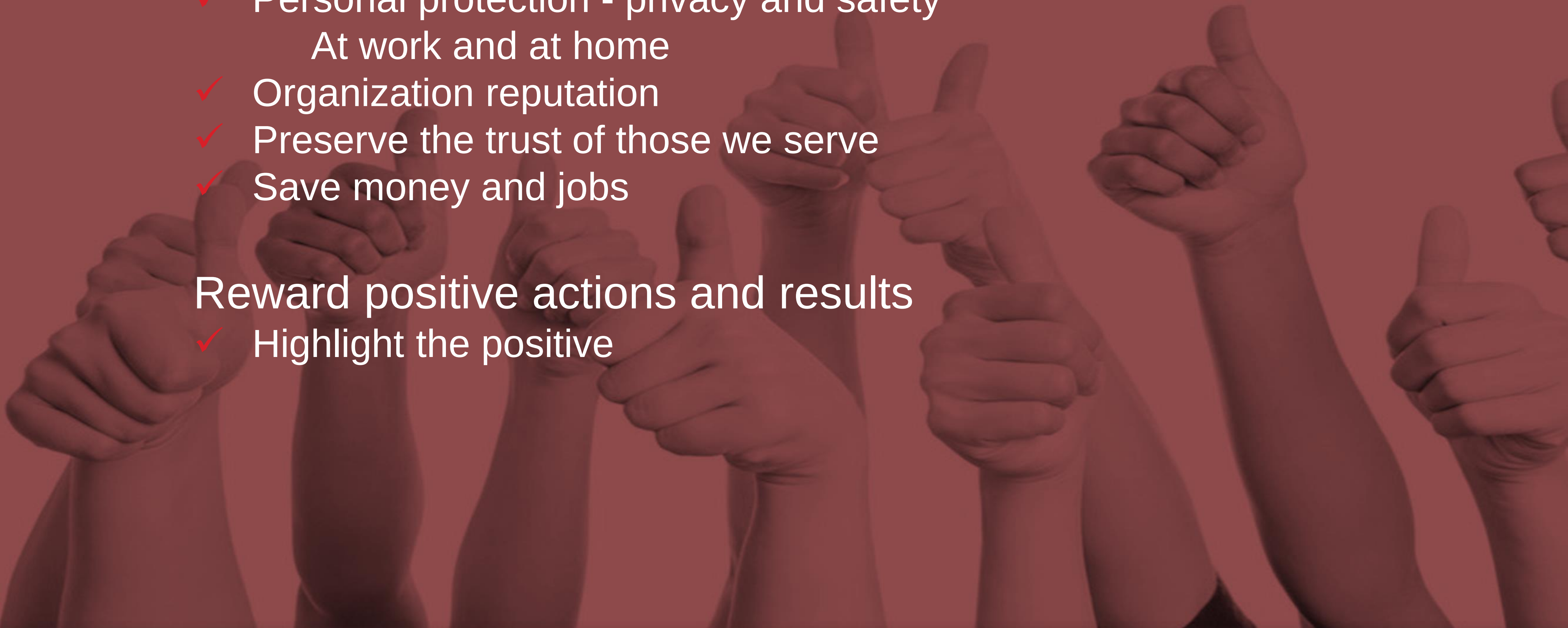


Function		Category		People	Process	Technology
ID	Identify	ID.AM	Asset Management	Applies	Applies	Applies
		ID.BE	Business Environment	Applies	Applies	
		ID.GV	Governance	Applies	Applies	
		ID.RA	Risk Assessment	Applies	Applies	Applies
		ID.RM	Risk Management Strategy	Applies	Applies	
PR	Protect	PR.AC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

- **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!

© 2015 Cisco and/or its affiliates. All rig

Thank You

cisco

Homeland Security

Creating a Culture of Cybersecurity at Work

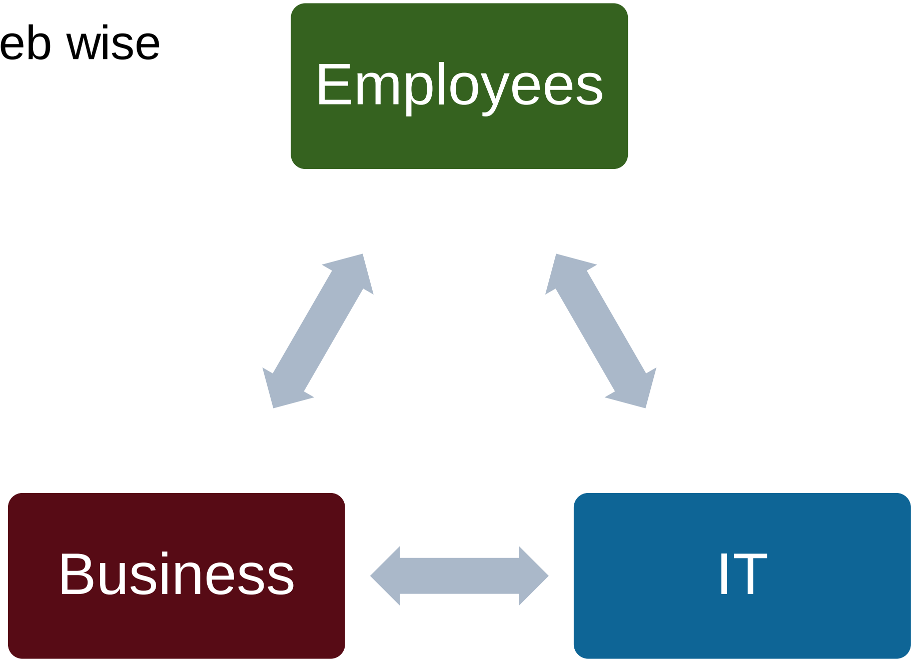
Benjamin Scribner
Department of Homeland Security (DHS)
National Cybersecurity Education & Awareness Branch (CE&A)

October 2015
National Association of Counties (NACo) NCSAM Webinar

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

For Business and Employees participate

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:

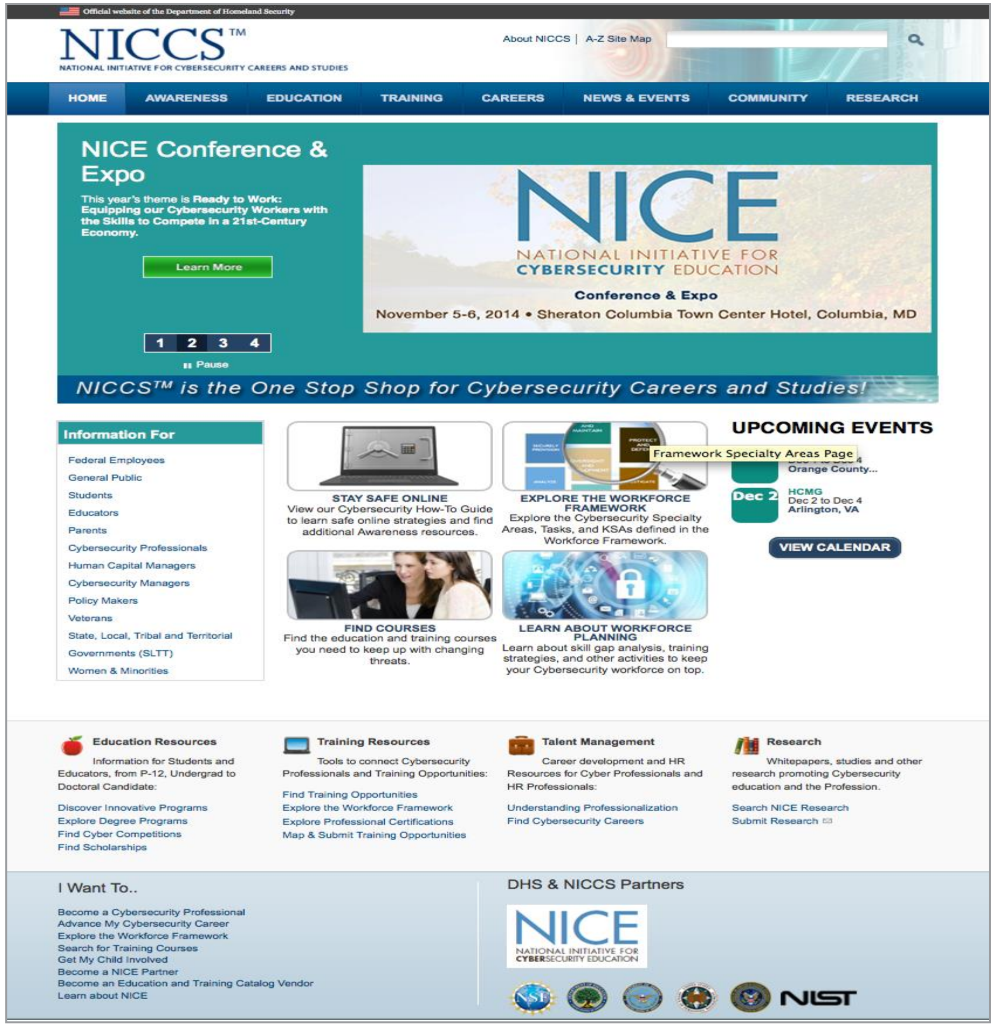
- **dhs.gov/national-cyber-security-awareness-month**
- **StaySafeOnline.org/ncsam**

For Business and IT goto NICCS

niccs.us-cert.gov

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

Questions? contact : **NICCS@hq.dhs.gov**



Official website of the Department of Homeland Security

NICCS™

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

About NICCS | A-Z Site Map

HOME AWARENESS EDUCATION TRAINING CAREERS NEWS & EVENTS COMMUNITY RESEARCH

NICE Conference & Expo

This year's theme is **Ready to Work: Equipping our Cybersecurity Workers with the Skills to Compete in a 21st-Century Economy.**

Learn More

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Conference & Expo

November 5-6, 2014 • Sheraton Columbia Town Center Hotel, Columbia, MD

1 2 3 4

Pause

NICCS™ is the One Stop Shop for Cybersecurity Careers and Studies!

Information For

Federal Employees
General Public
Students
Educators
Parents
Cybersecurity Professionals
Human Capital Managers
Cybersecurity Managers
Policy Makers
Veterans
State, Local, Tribal and Territorial Governments (SLTT)
Women & Minorities

STAY SAFE ONLINE
View our Cybersecurity How-To Guide to learn safe online strategies and find additional Awareness resources.

EXPLORE THE WORKFORCE FRAMEWORK
Explore the Cybersecurity Specialty Areas, Tasks, and KSAs defined in the Workforce Framework.

Framework Specialty Areas Page

FIND COURSES
Find the education and training courses you need to keep up with changing threats.

LEARN ABOUT WORKFORCE PLANNING
Learn about skill gap analysis, training strategies, and other activities to keep your Cybersecurity workforce on top.

UPCOMING EVENTS

Orange County...

Dec 2 HCMG
Dec 2 to Dec 4
Arlington, VA

VIEW CALENDAR

Education Resources
Information for Students and Educators, from P-12, Undergrad to Doctoral Candidate:
Discover Innovative Programs
Explore Degree Programs
Find Cyber Competitions
Find Scholarships

Training Resources
Tools to connect Cybersecurity Professionals and Training Opportunities:
Find Training Opportunities
Explore the Workforce Framework
Explore Professional Certifications
Map & Submit Training Opportunities

Talent Management
Career development and HR Resources for Cyber Professionals and HR Professionals:
Understanding Professionalization
Find Cybersecurity Careers

Research
Whitepapers, studies and other research promoting Cybersecurity education and the Profession.
Search NICE Research
Submit Research

I Want To..

Become a Cybersecurity Professional
Advance My Cybersecurity Career
Explore the Workforce Framework
Search for Training Courses
Get My Child Involved
Become a NICE Partner
Become an Education and Training Catalog Vendor
Learn about NICE

DHS & NICCS Partners

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

NIST

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