Countering Emerging Threats with an Effective Awareness Program

Karen S. Urban, CISSP

Federal Information Systems Security Educators' Association (FISSEA)
27th Annual Conference | March 18, 2014

K2SHARE

Evolving Technology

- Personnel expect greater mobility, connectivity, and networking capabilities
- As a result, networks today are a mixture of organizational issued and personally owned smart phones, tablets, laptops and desktop systems

K2SHARE

The Threat Landscape

Today cyber attacks on private, public and government information systems are organized, disciplined, aggressive, sophisticated, and are becoming all too common

K2SHARE

Personnel = Vulnerability

Whether intentional or not, organizational personnel continue to be a leading cause of data breaches and network intrusions

36% Of breaches were caused by inadvertent misuse of data by employees*

K2SHARE

*Forrester's "Understand the State of Data Security and Privacy Report"

P@s5w0rd$

76%

of network intrusions exploited weak or stolen credentials*

K2SHARE

*Verizon 2013 Data Breach Investigations Report
Image above courtesy of SplashData

Willingness to "Click"

1	Spear Phishing Attack		Fake emails masquerading as legitimate correspondence are sent to targeted users.
2	Malware Installed		The user clicks on a link or opens an attachment. Malware is executed and installed on the user's computer.
3	Privilege Escalation		The attacker uses the malware to escalate their privileges. Access is gained to passwords and other systems.
4	Data Extraction		Data gathered from end user workstations, servers and databases is transmitted back to the attacker through the Internet.

K2SHARE

Good Intentions, Bad Results

Dropbox

MediaFire

Gmail by Google

Google Drive

Microsoft® SkyDrive®

YAHOO! MAIL

Unauthorized
File Transfers

K2SHARE

Social Media Oversharing

K2SHARE

How to Defend Against Ourselves

Implement, lead and sustain an active and aware cybersecurity culture!

K2SHARE

Cyber Security Awareness Program

- Identify and target vulnerabilities introduced by human behavior
- Include real-life scenarios which people may actually encounter at work and at home
- Vary your delivery to capture and retain attention considering the range of learning styles that exist today
- Utilize metrics to measure effectiveness over time

Identify & Target Vulnerabilities Introduced by Human Behavior

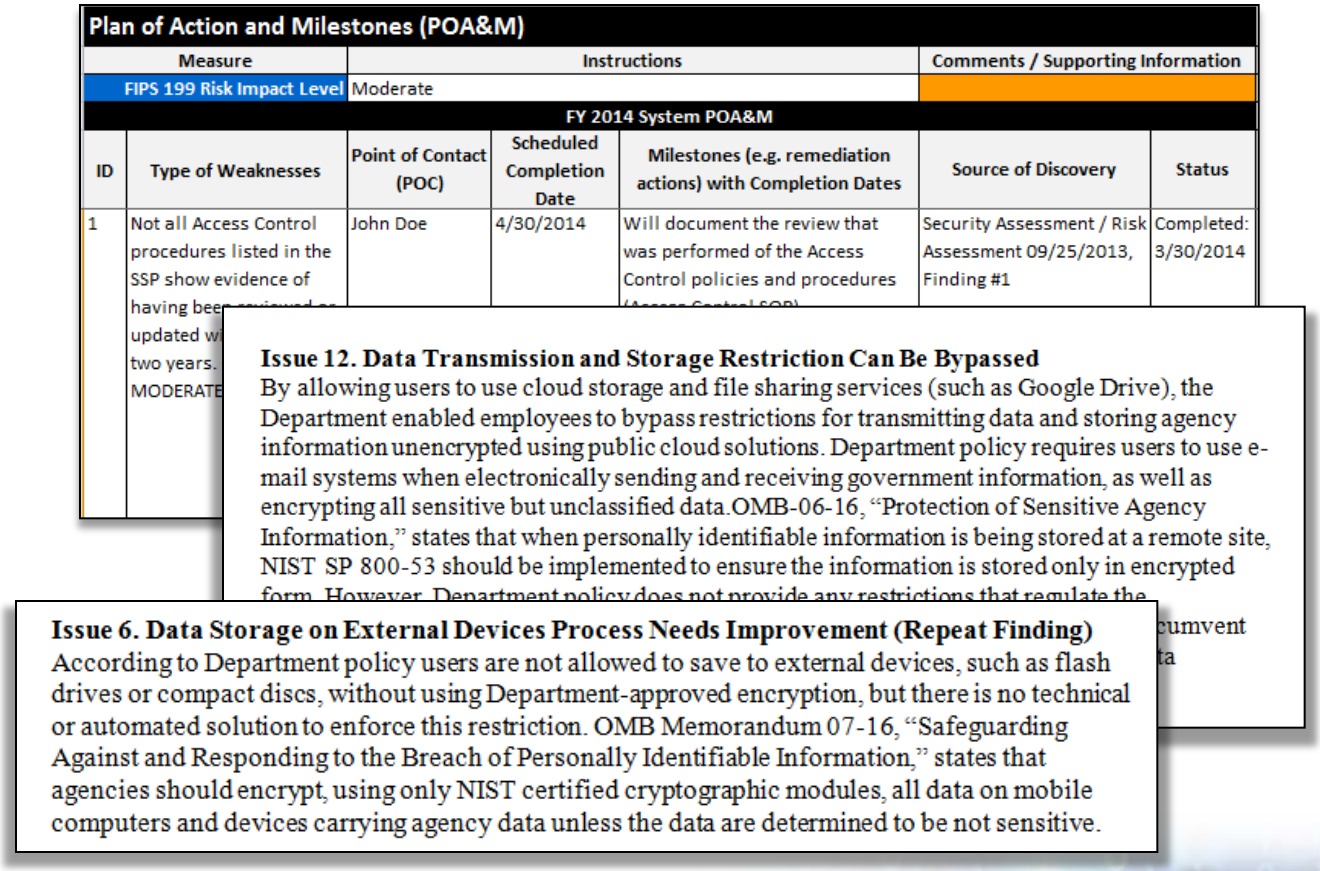
- Analyze information contained in security incident reports, audit reports and Plans of Action & Milestones (POA&M)
- Examine organizational Policies and Procedures
- Consult with organizational Security and Privacy Subject Matter Experts (SMEs)
- Develop or Update a Security Awareness Baseline

Incident Reports

- Partner with members of your Security Operations Center and Incident Response Teams
- Analyze incident reports to identify incidents where the **root cause** was human behavior

Audit Reports and POA&Ms

- A closer look often reveals the root cause is human behavior
- Awareness training should be considered – even when a technical solution is recommended



Plan of Action and Milestones (POA&M)

Measure	Instructions	Comments / Supporting Information
FIPS 199 Risk Impact Level	Moderate	

FY 2014 System POA&M

ID	Type of Weaknesses	Point of Contact (POC)	Scheduled Completion Date	Milestones (e.g. remediation actions) with Completion Dates	Source of Discovery	Status
1	Not all Access Control procedures listed in the SSP show evidence of having bee… updated w… two years. MODERATE	John Doe	4/30/2014	Will document the review that was performed of the Access Control policies and procedures (Access Control SOP)	Security Assessment / Risk Assessment 09/25/2013, Finding #1	Completed: 3/30/2014

Issue 12. Data Transmission and Storage Restriction Can Be Bypassed
By allowing users to use cloud storage and file sharing services (such as Google Drive), the Department enabled employees to bypass restrictions for transmitting data and storing agency information unencrypted using public cloud solutions. Department policy requires users to use e-mail systems when electronically sending and receiving government information, as well as encrypting all sensitive but unclassified data.OMB-06-16, "Protection of Sensitive Agency Information," states that when personally identifiable information is being stored at a remote site, NIST SP 800-53 should be implemented to ensure the information is stored only in encrypted form. However, Department policy does not provide any restrictions that regulate the…

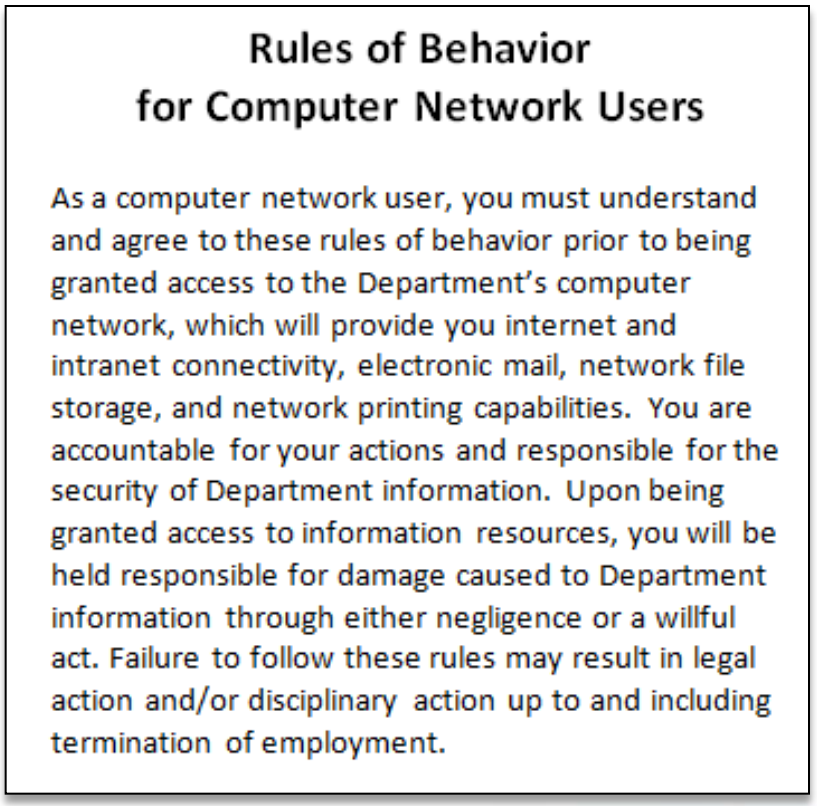
Issue 6. Data Storage on External Devices Process Needs Improvement (Repeat Finding)
According to Department policy users are not allowed to save to external devices, such as flash drives or compact discs, without using Department-approved encryption, but there is no technical or automated solution to enforce this restriction. OMB Memorandum 07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," states that agencies should encrypt, using only NIST certified cryptographic modules, all data on mobile computers and devices carrying agency data unless the data are determined to be not sensitive.

…cumvent …ta

K2SHARE

Policies and Procedures

- Identify potential gaps between requirements and actual implementation
- Review your Rules of Behavior (RoB)
- Consistent message between the awareness training program and other training



Rules of Behavior
for Computer Network Users

As a computer network user, you must understand and agree to these rules of behavior prior to being granted access to the Department's computer network, which will provide you internet and intranet connectivity, electronic mail, network file storage, and network printing capabilities. You are accountable for your actions and responsible for the security of Department information. Upon being granted access to information resources, you will be held responsible for damage caused to Department information through either negligence or a willful act. Failure to follow these rules may result in legal action and/or disciplinary action up to and including termination of employment.

K2SHARE

Consult with Security & Privacy SMEs

Gain insight to:

- Organizational strategies to mitigate risk
- New or updated policies and procedures

K2SHARE

Develop or Update a Security Awareness Baseline

- Survey your personnel:
  - ✓ Identify areas where awareness is lacking or perceived challenges exist
  - ✓ Find out what they think will help them "behave in" instead of "behave out"
- Perform phishing exercises
- Informal outreach sessions

Learning Styles & Culture

- Telling is not learning
- E-reading (PowerPoint and e-learning as fancy PowerPoint) is not very effective except as an easy way to "check a box"
- Training only happens when the learner is "training" themselves, i.e., they must focus on the training to progress; they must engage with problem solving; and they must have repeated practice using gained knowledge and skills

Use Real-life Scenarios

- Training must be relevant to the learner
- Use real-life scenarios
- The more they can relate to and experience the scenario the more effectively they will remember what is being taught

K2SHARE

Metrics & Continuous Monitoring

- Don't try to focus on everything; focus a few problem areas at a time!
- Deliver training more often (not only once a year) so you can address more topics throughout the year and based on real metrics

Use metrics like these to track progress and measure impact:

# of personnel that successfully pass phishing exercises

# of personnel that didn't pass phishing exercises

# of personnel that report receipt of a phishing exercise email

# of actual phishing incidents

# of malware infected systems

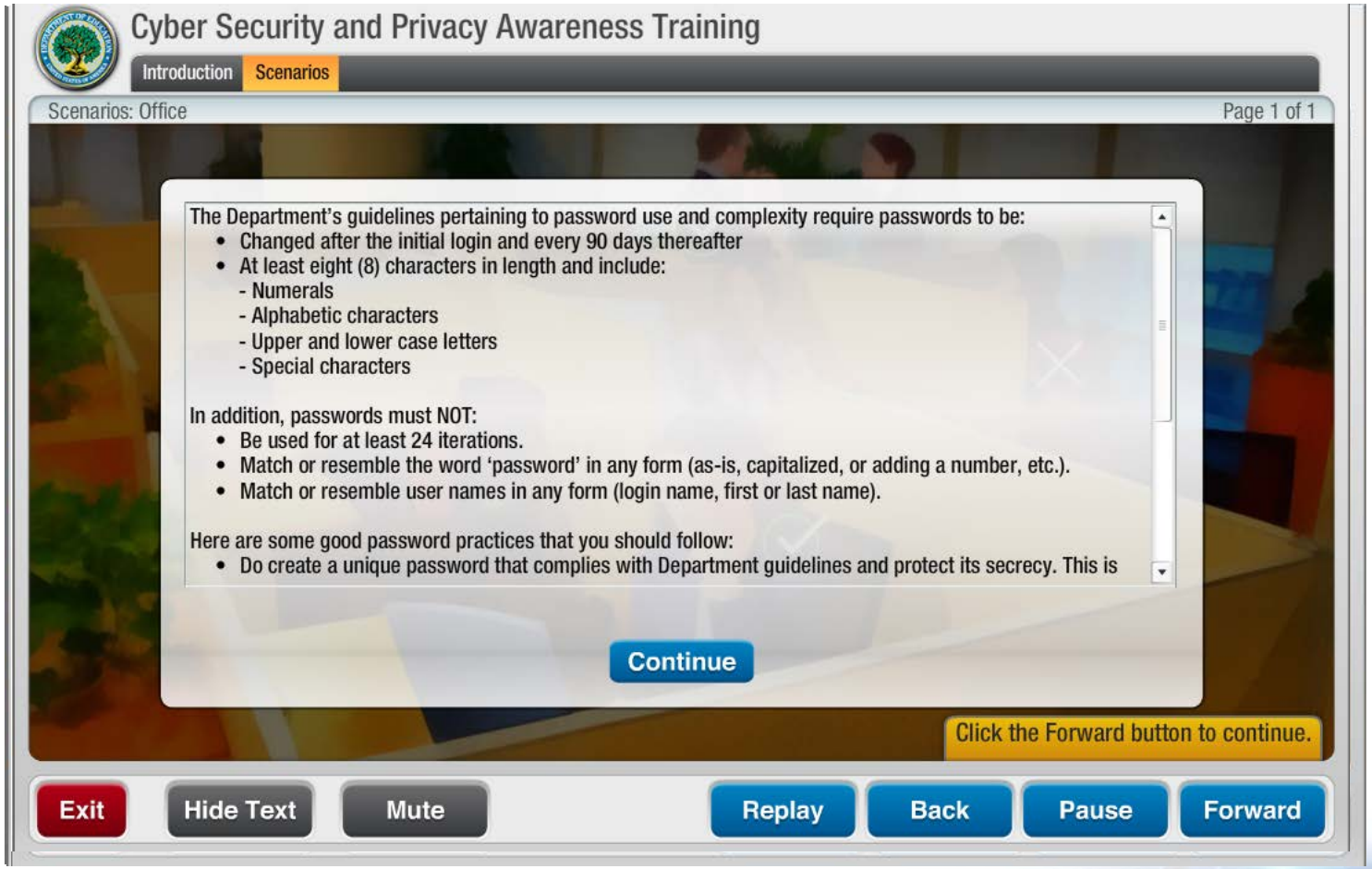
K2SHARE

Putting These Concepts to Work

The Department of Education's FY 2014 Cyber Security & Privacy Awareness Course

K2SHARE

Real-life Scenarios in Action



K2SHARE

Repeat to Reinforce

K2SHARE

Questions

For additional information, please contact:

Karen S. Urban

PMP, CISSP, CISA, CRISC, GPEN
Program Manager
M 979.220.6810 | O 979.260.0030

Larry D. Teverbaugh, Ph.D., PE

President & CEO
M 979.777.1127 | O 979.260.0030

http://www.k2share.com | Veteran Owned Small Business

K2SHARE