“Use News”
to build your awareness program

2011 FISSEA Conference
David Kurtz
Bureau of the Public Debt
Public Debt’s Program

• Orientation, End User class, annual DoD tutorial
• Not just once a year – multiple conveyances
• Emphasis on real news and lessons learned
• FrontLine Newsletter (quarterly)
• ISSR Newsletter (monthly)
• Monthly Security Reminders on intranet
• In-house magazine (Security Spotlight column)
• [Even some posters come from real stories]
FrontLine Newsletter

- Computer Security Institute (www.GoCSI.com)
- Quarterly four-page newsletter (since the ‘90s)
- Good articles cover all major security topics
- Because of external source, it may have an aura as an accredited expert telling us what to know
- Sent to all employees (now through TLMS)
- Last page always contains local information
- Annual subscription costs $1,860
ISSR Newsletter

• Distributed monthly to all ISSRs, who forward to everyone in their areas (can customize)
• Simple text e-mail of about 1200-1500 words
• Always starts with teaser for Monthly Security Reminder, followed by a review of one item from the IT Rules of Behavior
• Contains a variety of news items, both from internal and external sources
Monthly Security Reminders

• Appear prominently on intranet home page
• Longer than typically used in the ISSR Newsletter (released the same day)
• Added to “The Security Zone” archive
• Easier to incorporate screen shots or other color graphics (e.g., pictures of ATM skimmers)
• Often with intriguing titles to arouse curiosity
  *(Take a peek at a leak; Trash talkin’; Men are better than women?; Flashing; Three heroes)*
Security Spotlight

• “Of Interest” is Public Debt’s official quarterly newsletter
• Sent to all employees, plus some retirees
• Joint effort with Physical Security (split load)
• Longer articles (~500 words) sometimes with good tips for home users
How do you come up with enough content for all these publications?
Get Connected!

Establish relationships with

- PC Support
- E-mail Admins
- Helpdesk
- Other Technical Gurus (including Pen Testers)
- Disaster Recovery
- Physical Security
- Procurement & Travel Credit Cards
- HR
- Janitors
- FISSEA (*lots of ideas have been stolen here*)
CSIRC

Computer Security Incident Response Capability (CSIRC) required by NIST

- Reacts and investigates all incidents, and submits reports to Treasury
- Handles anything from a lost Blackberry to a major breach
- CSIRC reports provide excellent learning opportunities to avoid future incidents
Virus Victims

[An alert is sent whenever malware is discovered, so get put on the list to get this notification]

• Standard letter sent to all virus victims (cc: to ISSR)
• Emphasizes learning from each other
• Provides links to previous victim stories
• Offers anonymity in the newsletter
• Encourages further training
• Not a disciplinary letter and no required response
• Provides some incentive to avoid becoming another virus victim story
Pastwords

• Articles on password strategies from retirees
• Notified by HR prior to departure
• Standardized letter sent encouraging them to share how they created passwords
• The retiree is not named
• Provides creative insights into password strategies of coworkers, which hopefully translates into more robust passwords
RoB & History

• One regular feature we include is to review a selection from our Rules of Behavior
• Another source for stories is your agency’s own history
• Refer back to previous articles by creating an archive of prior publications on your intranet, and then tie current events into past situations
Feedback Loop

• Be sure to provide a way for employees to contact you to provide story ideas
• Actively seek internal stories, because they are the most interesting, and help to lead to more story ideas (including stories from home)
• Another way to promote readership is to hide rewards within the text of the article (*the first 100 employees who read this get a gold coin*)
State Dept. Awareness

- Thrice weekly newsletter entitled “In Case You Missed It” covering security issues
- Includes a brief summary, plus links for more information
- For your free subscription, send a request from a .gov or .mil account with the subject line "Subscribe" to awareness@state.gov
- Excellent source of potential news stories

[If there aren’t enough lessons to be learned from your own place, use someone else’s lessons!]
Other Useful Sources

This is a partial list of potential newsletter article sources (but not an official endorsement):

- www.sans.org – Ouch & NewsBites newsletters
- http://nakedsecurity.sophos.com/
- http://krebsonsecurity.com/
- http://www.schneier.com/
- http://www.wired.com/threatlevel/
- http://blogs.pcmag.com/securitywatch/
- http://blog.trendmicro.com/
- Plus many, many more!
Summary

• Once a year tutorial is not enough!
• Newsletters provide an easy vehicle to increase employee awareness to current security issues
• Important to establish “linkages” with potential news sources (internally and externally)
• News about real incidents within your organization is interesting – learn from mistakes!
• There are lots of security stories, so share them with your employees (*often helpful at home, too*)

David Kurtz • (304) 480-7979 • david.kurtz(at)bpd.treas(dot)gov