

## **CIC CIO TechForum 2007**

Wednesday, October 3

“How Purdue University Delivered a More Secure IT Work Environment for their Enterprise Application (EA) Development Staff”

by Melissa Burton, PMP & Brian York, MBA, PMP

*Thank you for letting us present our security projects.*

# How do we protect our Information Assets & Employees while supporting Enterprise Applications?

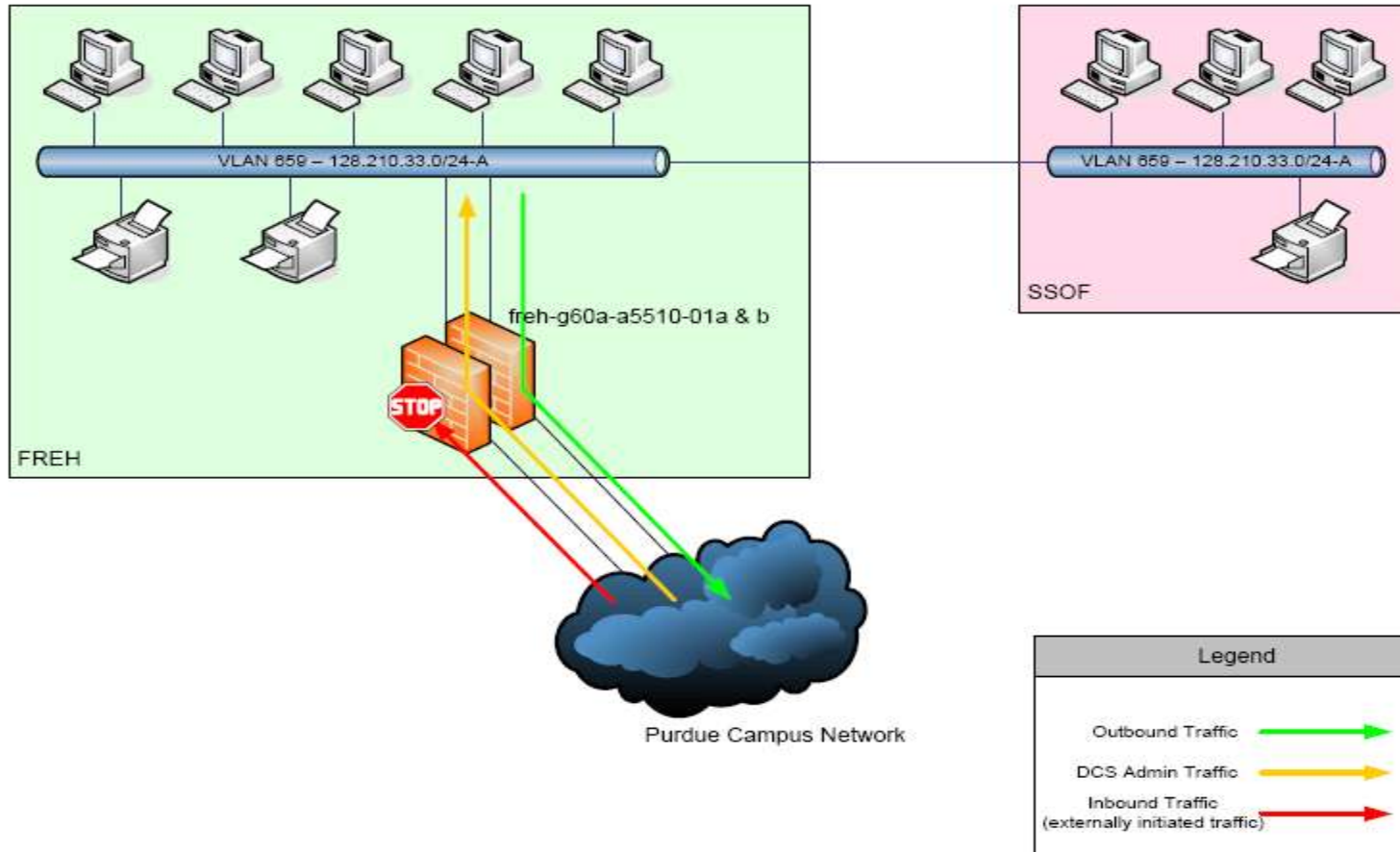


# Purdue's Enterprise Application Department Security Projects

Melissa managed a Firewall Project that; consistent with the OnePurdue initiative, moved all ITEA staff (management, OSS, and developers) workstations behind a development firewall. In the future, this firewall might be scaleable to other ITaP developers, but the need in ITEA was urgent because of the nature of the unit's mission and work.

Brian managed a Security Awareness Project to establish an environment where every EA employee is data and workstation security conscious and executes work in a secure manner.

# ITEA Firewall Implementation



# ITEA Firewall Project

## ❖ Sponsors

- Jeff Whitten, Associate Vice President of IT Enterprise Application
- Mike Carr, Chief Information Security Officer



# ITEA Firewall Project

## ❖ Other Resources Involved

- Project Manager, ITEA
- ITEA Developers
- Desktop Computing Resource
- Network Resource
- Security Resource



# Firewall Goal/Objectives

**Project Goal**

Move all IT Enterprise Application staff workstations behind a development firewall.

**Project Objectives**

1. Move entire department to one subnet
2. Determine what ITEA staff need access to external resources that are IP restricted
3. Assign static IPs to all ITEA staff
4. Select Firewall option
5. Purchase Firewall server
6. Implement Firewall
7. Plan Firewall maintenance
8. Establish an SLA with IT Networks and Security to assure service if the Firewall unit breaks

# Firewall Key Requirements

- ❖ There will be no inbound access. An exception will be made for DCS patch installation, vulnerability scanning, and viral scanning.
- ❖ There will be no outbound service rules set up.
- ❖ Failover requirements: It is recommended that the firewall be fully redundant.
- ❖ Physical location of firewall should be housed in FREH.
- ❖ The firewall should be implemented after all of ITEA have moved to static IP addresses.



# Project Execution Milestones

- ❖ **Select Firewall hardware and complete purchase requisition**
- ❖ **Receive and install Firewall device**
- ❖ **Determine options for in-bound access**
- ❖ **Create test plans for mainframe and open systems**
- ❖ **Create Rollback Plan**
- ❖ **Ensure ITEA staff have been assigned a static IP**



# Project Execution Milestones – Continued

- ❖ Add new rules to other Firewalls EA staff are going through
- ❖ Build Firewall rule sets - Security
- ❖ Move ITEA testers behind Firewall
- ❖ Create/Distribute Firewall Project Flyer to EA staff
- ❖ Firewall Access Management
- ❖ Complete Service Level Agreement with Networking and Security
- ❖ Move all ITEA staff behind Firewall



# Major Lessons Learned

- ❖ Helpful having reps from all parties involved and committed to the project
- ❖ Testers had the technical knowledge to provide good feedback
- ❖ Initially migrate 1 tester versus the entire test group
- ❖ Accurate list of ITEA workstations, IPs, PICs, MAC addresses
- ❖ Accurate list of IP restricted servers



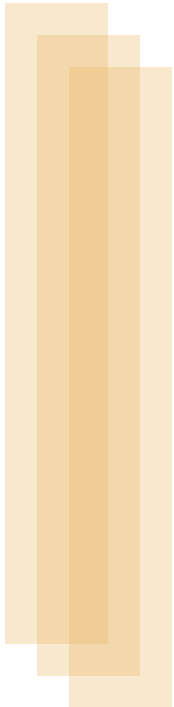
# Quote from Sponsor

- ❖ "Like many IT shops, our developers have been forced to transition from monolithic mainframe development environments to multi-tiered client/server and web development environments. Tools in these new environments present new security risks. Our developers' firewall and security awareness projects sought to create a more secure development environment for staff. The success of these projects has been a critical success factor in the 'SecurePurdue' initiative." --*Jeff Whitten, Associate Vice President of IT Enterprise Application*

# ITEA Security Awareness Project

- ❖ Executive Sponsor – Brad Skiles,  
Director, Enterprise Shared Services
- ❖ Sponsor – Nancy Yuochunas,  
Director, Business Services Applications

# Mission Statement



Security has become an increasingly important issue in Purdue's technology environment. Each department has a responsibility to provide their staff with the information and resources that they need in order to fulfill their obligations of ensuring the security of Purdue's data and computing environment.

# Project Objectives

- ❖ **Establish an on-going EA Security Awareness Program that includes but is not limited to:**
  - **University access and authentication policies and best practices**
  - **Indiana legislation regarding Social Security Number and other sensitive data**
  - **FERPA, GLBA and HIPPA guidelines**
  - **Data classification, handling and disposal guidelines**
  - **Testing & Application Security best practices**
  - **Periodic individual reviews and/or security awareness “certifications”**
- ❖ **Identify and establish a single security point of contact.**

# Key Requirements

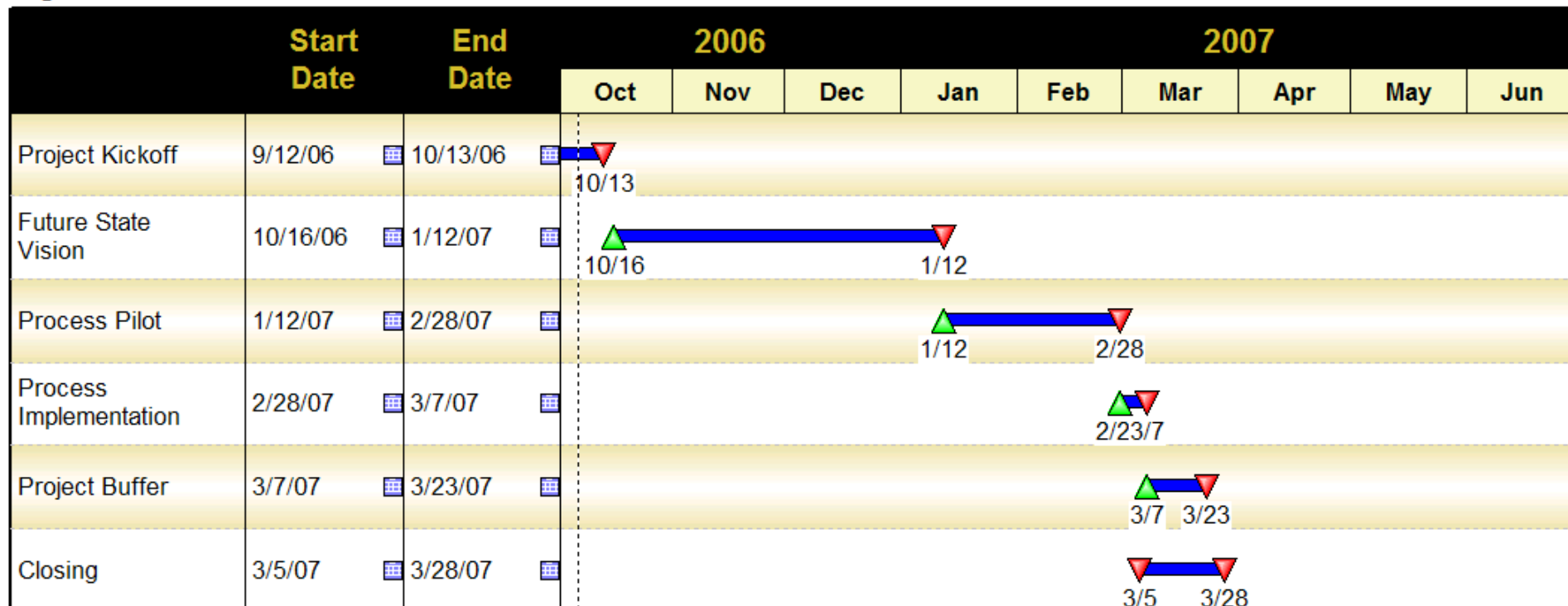
- ❖ Development of a sustaining program
- ❖ Creation of multiple channels of effective data and workstation security communications
- ❖ Establishment of a direct communication channel to IT Security
- ❖ Maintain the data and workstation security knowledge already gathered
- ❖ Leverage the completed work of IT Security



# Scheduled Work

## EA Security Awareness Project

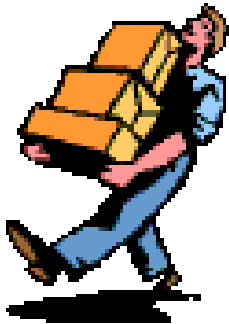
Page 1 of 1



Resource Constraint: 3 Analyst/Programmer's 20% allocation each in addition to the project manager

# Major Products Delivered

- ❖ ITEA Security Awareness Committee (Standing)
- ❖ Security Procedures Reference
- ❖ WebCT Vista Security Assessment



# ITEA Security Awareness Committee

- ❖ Maintains a general state of awareness of security concerns
- ❖ Permanent Chair – EA Security Contact
- ❖ Three (3) members who represent a cross-section of the department
- ❖ Duties and responsibilities to be shared equally by committee members
  - Interface directly with IT Security
  - Identify and document sources of security awareness credits
  - Track EA employee security awareness credits
  - Draft and disperse, via multiple methods, messages to maintain security awareness
  - Update any 'living' documents as appropriate
  - Advise, conduct, or organize EA specific security-related forums, training or workshops

# Security Procedures Reference

## ❖ Major Topics Covered

### ➤ Policy, Practices and Prevention

- Data classification and handling
- Resource usage
- Application development and maintenance
- Responsibilities

### ➤ Response

- Incident
- Disaster recovery
- Spam

## ❖ Published on departmental “Commons” Website

# WebCT Vista Security Assessment

- ❖ Team drafted 74 Security Awareness Assessment Questions and Answers
- ❖ Reviewed by IT Security
- ❖ Assessment Questions Loaded into Vista for employee assessment



# What could have gone better?

- ❖ MS Word Document Merge
  - Lost and messed-up some documents by allowing Word to merge versions
  - Just say “No” when Word asks if it can merge versions
- ❖ Staff reassignment to OnePurdue (before project work was complete)
- ❖ Needed a communications point person with Desktop Computing Support

# Sponsor Observations

- ❖ “The project illustrated management's commitment to security and our desire to help provide staff with the information they need to protect the University and themselves.”
- ❖ “It was a wonderful example of cross unit/departmental cooperation.”
- ❖ “The reference manual is a quality, professional document that also provides a framework for communicating new or changed security information and procedures.”
- ❖ “Concerned that our workload and organizational changes/transitions have impacted the formation of the security committee and therefore our ability to make security activity a natural, recurring part of our everyday professional lives. Hopefully there will be an opportunity to move forward with this in the near future.”

--Nancy Yuochunas, Director, Business Services Applications

# Final Comments

❖ Questions?

❖ Contact Information

- Melissa Burton – [maburton@purdue.edu](mailto:maburton@purdue.edu)
- Brian York – [bryork@purdue.edu](mailto:bryork@purdue.edu)