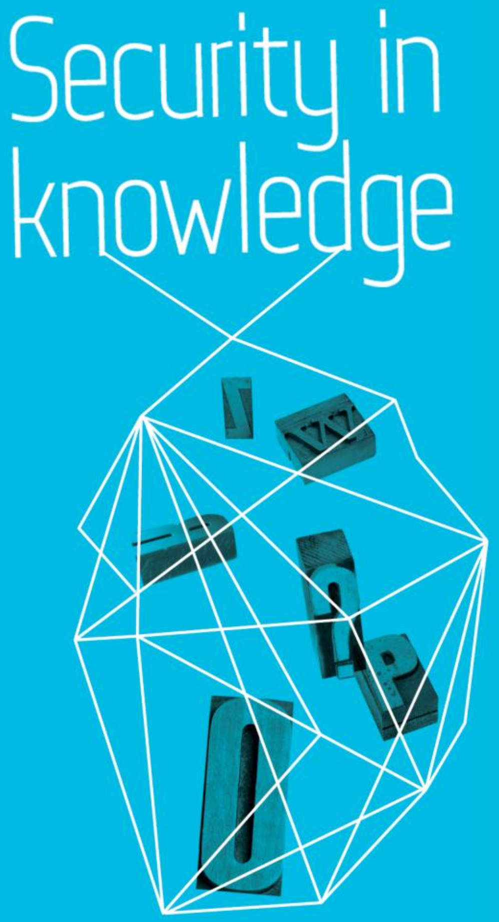
RSACONFERENCE2013



DO YOUR BUSINESS PARTNERS’ WEB SITES PUT YOU AT RISK?

Ann L. Wolf, CISSP

The Board of Pensions PCUSA

Session ID: ASEC-F43

Session Classification: Intermediate

Trust but Verify

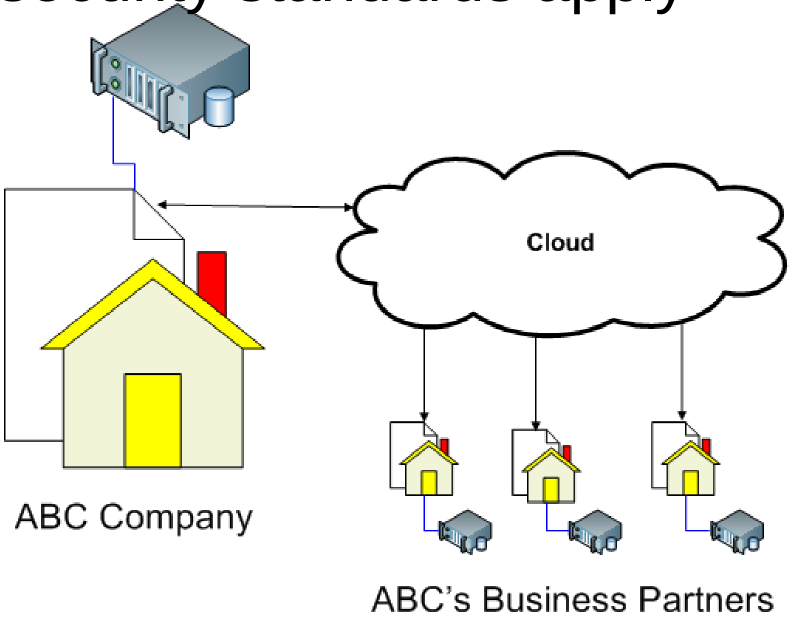
- Trust intentions but verify controls
- WhiteHat Security reported in 2011
  - On average, a web site in 2011 had 79 vulnerabilities*
- Verizon's 2012 Data Breach Investigation Report noted**
  - 92% incidents discovered by third parties

*http://www.slideshare.net/jeremiahgrossman/stat-swebinar062712

** http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

Data is Outside of Our Controls

- Business partners provide services for your clients
- Client data shared with and created by business partner
- Cannot presume the same security standards apply
- Trust, but verify



Options to Minimize Risk

1. Obtain cyber insurance
2. Review IT general controls
   - Review independent audit reports (e.g. SSAE)
   - Questionnaires and interviews
3. Review web site controls
   - Questionnaires and interviews
   - Test web site security
4. Detailed independent audit and penetration test

Frequent Issues Noted

- First review completed 2001
- Business goal is to provide services
- Issues noted in 1 of 3 reviews completed
- Frequently noted issues
    - The authentication process is not encrypted
    - The account lockout process does not work
    - Search criteria in URLs is not encrypted and can be changed
    - Data input controls are weak or non-existent
    - Confidential data is saved in cached files

What Is Needed

- Standard – review initial security setup of linked websites
- Review of security controls and functionality
- Similar aspects to audit and quality assurance reviews
- Not ethical hacking or penetration testing
- Outcome – balance business requirements with risk

The Review Process

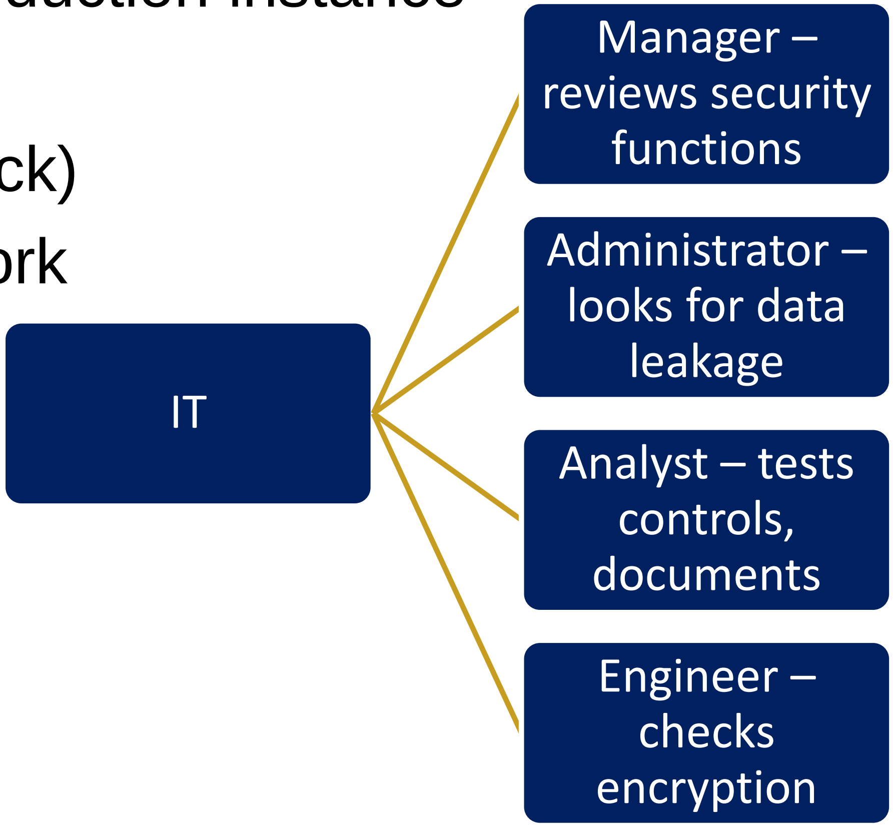
- Start with Quick Review and Questions
  - No hands-on testing is done
  - Interview business partner’s staff
  - Observe web site when possible
  - Review access, data and preventative controls
- Decision – Stop Here or Continue?

Review List
Privacy policy ☑
Account timeout ☑
Encryption used ☑

Your quick review guide and questions are in the bonus slides

Hands-on Review

- Get access to a non-production instance
- Follow the user’s path
- Review and test (not hack)
- Verify stated controls work
- Check for cached data



IT

Manager – reviews security functions

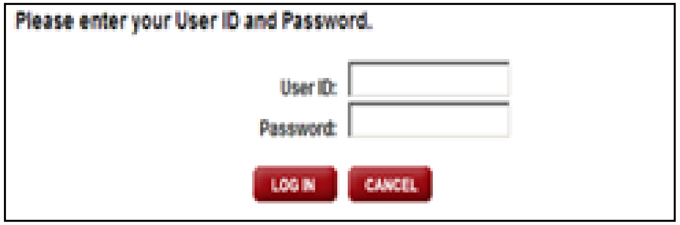
Administrator – looks for data leakage

Analyst – tests controls, documents

Engineer – checks encryption

Hands-on Review – Create an Account

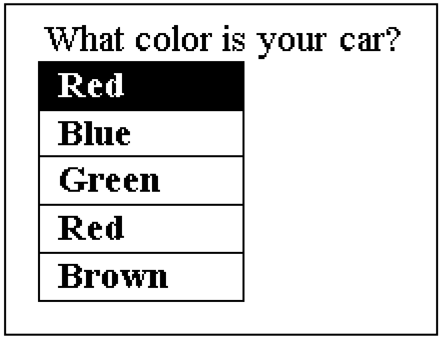
- Test that the controls actually work
  - Create an account and check
    - Data requirements
    - Data controls
  - Access the account and check
    - Invalid attempts and locking of the account
    - Password requirements
    - If codes are used, try guessing codes



Please enter your User ID and Password.

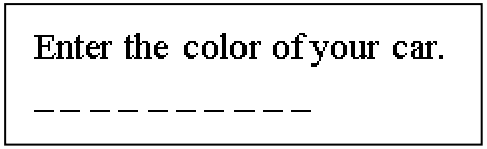
Hands-on Review – Use the Account

- Compare the controls to a similar website
- Check data entry design and test controls


What color is your car?

- Red
- Blue
- Green
- Red
- Brown

Vs.


Enter the color of your car.

_ _ _ _ _ _ _ _ _ _ _

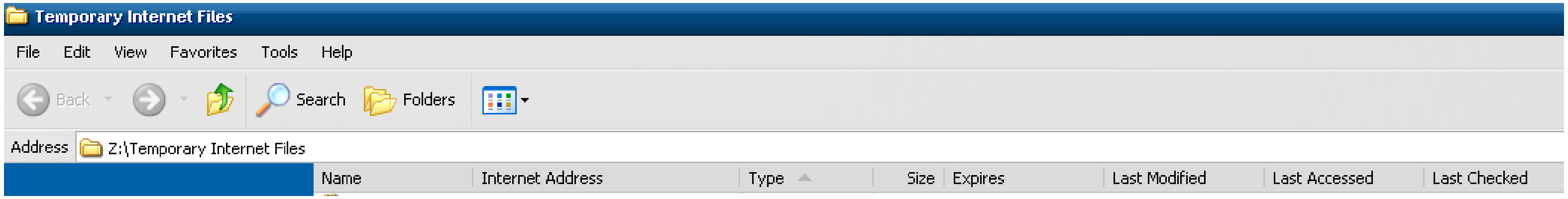
Hands-on Review – Use the Account

- Check data passed in URLs

https://www.mywebsite.org/createaccount.aspx?supplierURL=1234

- Save bookmarks, exit and try them

- Check cached files


Temporary Internet Files

Address Z:\Temporary Internet Files

The complete list is in the bonus slides

When You Have Results

- Begin negotiations
- Use your business team contacts
- Quantify the issues
  - Major, minor or a usability concern
- Minimize yelling “fire”

How to Apply What You Have Learned

- Within next three months – do one review
  - Contact your business, project or web services staff
  - Determine planned changes and current web services
  - Get started
    - Revise checklist provided for your use
    - Do a hands-on test & review results with your contacts
    - Follow-up on issues noted
- Within the year – make this a standard procedure
  - Change company standards to review all new business partners' web sites for your employees and customers
  - Review new sites – <u>before</u> implementation is ideal
  - Rank existing sites and determine if reviews are needed

Reduce Your Risk …

Trust, but Verify

- Start discussions with your business, project or web services staff
- Use the bonus slides from this presentation
- Review your business partners’ web sites
- Minimize your risk and protect your data

Questions?

- Contact Information
  - Ann L. Wolf, CISSP annwolf123@gmail.com

Bonus Slides

These slides are for the RSA attendees’ downloaded version only.

Quick Review Questions

Listed below are questions to be used as a guideline for a quick review of security controls over your business partners' web sites. In some cases, these web sites may process your customers' data or provide your customers with access to their data via the web.

1. Access Controls

What are the sign-on, access and authentication policies?

How does the user gain access to the site?

Is two-factor authorization available?

For staff access, how is access to special records controlled (such as other employees' records)?

For staff access, can the business partner limit access to your data by requesting IP number?

What are the rules over the passwords and PINs?

Following incorrect authorization attempts, when do accounts timeout? Is any password throttling done (increasing time after failed attempts)?

Is CAPTCHA used?

Are there mobile applications? How are they tested?

For customer related web sites, what prevents hackers from obtaining access to a user's data if the user does not access the site?

Is there an independent audit report available (such as a SSAE report or penetration test results)?

Is there a Privacy Statement on the website?

Is there decentralized security, to allow our security administrators to control our users' access to the web site?

Quick Review Questions

2. ***Preventative Security Controls***

   Who manages the application on the back-end?

   Where are the data centers and where physically is the data?

   Does the vendor’s staff have access to our data remotely? If so, what controls are in place?

   Does the vendor use thin client computing?

   Is there a host Intrusion Detection System or Intrusion Prevention System?

   How and when are network logs monitored?

   What policies are in place to detect and stop insider breaches and hacking attempts?

   Who handles penetration testing and how is it done?

   At what point will a user’s account become locked after invalid access attempts?

   How are invalid log on attempts monitored?

   What controls are in place to prevent SQL injection (such as input validation) and cross site scripting?

   What is the backup and recovery plan?

   What is the preferred file transfer protocol?

   How are files shared with our company?

Quick Review Questions

3. *Protected Healthcare Information, Personally Identifiable Information & Other Data*

How is the storage of our data separated from that of other customers?

What data is presented automatically and what data is optionally presented?

What encryption policies will protect data during transmission and storage?

Is there any confidential data passed in unencrypted URLs?

Is the data presented reasonable and necessary for the purpose of the web site?

How long is the data cached in memory?

If the user exits the site, is the information available via the Back button? If so, for how long?

If the user does not log off, when will the session be timed out?

Are there any free text input fields on unencrypted pages in which a customer could incorrectly enter PHI or PII?

4. *Marketing (if the web site is accessible by customers)*

What web sites are linked via the web site being reviewed? Are these acceptable?

Is the information presented on the web site being reviewed correct for our customers and/or employees?

Hands-on Review

Listed below are test steps to review the security controls over your business partners' web sites. In general, you should test the site as though you were a user. If users can create their own accounts, start with that step and then proceed to the review security over the web site's functional access. If any issues are noted, screen print (electronically) the screens and any messages received.

1. *Initial User Access*

Read the privacy statement and other similar statements (such as terms and conditions, help and security statements). If no privacy statement is posted, note this as an issue.

If the site provides the functionality, create an account.

Try leaving required field blank, one at a time.

Test the password (or other authentication controls).

Test a valid user ID and password combination.

Test an invalid user ID.

Test a valid user ID and invalid password

Enter invalid passwords to lock the account.

Did the account lock when expected? If the account unlocks automatically, does it work as expected?

Test the password controls work as expected.

If there is a forgotten password capability, is there a single key (correct match) for the questions and answers?

If company codes are used to create an account, try guessing other codes. (You want to test if someone could easily hack into YOUR company's data.) If you are successful, print the screen and STOP with this test step.

Hands-on Review

2. ***Using the Website***

   Try to cause data entry errors. If you get any, do they provide any confidential system information?

   Check the encryption certificate details. Is a lock symbol visible? Is the URL an https address? Make sure the certificate is valid and has not expired. Check the level of the certificate. Compared to other web sites, is it sufficient?

   Check the web site’s functionality with a security view.

   If file or picture uploads are permitted, review and test the controls over the file types, number of file uploads, and size permitted.

   Bookmark pages and attempt access without the standard authentication controls.

   Check data entry design and test controls to determine if there are data controls (such as zip code field can only be numbers). Drop down menus and radio buttons are generally better than fields allowing free form entry. If controls are not provided, the database may be at risk of SQL injection. Do not enter malicious data.

   Review the Temporary Internet Files and cookies for any cached files with confidential data.

      Check saved PDF, TIF and HTML pages. Sort by type, by date and by site.

   Using any saved HTML pages, test if the authentication controls can be bypassed to access the secured pages.

   If the URL links are not encrypted, changed the data in the URLs and test if you can access another account.

      STOP if you can (and save a screen print) and exit the site.