DRAFT 2012 UC Davis Cyber-Safety Survey

UNIT INFORMATION

Enter the following information.
Person completing report
Email
Phone
Unit (include sub-unit information, if appropriate)
College/School/Office
  College of Agricultural and Environmental Sciences
  College of Biological Sciences
  College of Engineering
  College of Letters and Science – Humanities, Arts and Cultural Studies
  College of Letters and Science – Mathematical and Physical Sciences
  College of Letters and Science – Social Sciences
  Graduate School of Management
  Information and Educational Technology
  Administrative and Resource Management
  Offices of the Chancellor and Provost
  Office of Graduate Studies
  Office of Research
  Office of Resource Management and Planning
  Office of Student Affairs
  School of Education
  School of Law
  School of Veterinary Medicine
  UC Davis Health System
  University Extension
  University Library
  University Relations

Enter the following general information about the computing environment in your unit.
Number of Windows Systems
Number of Macintosh Systems
Number of Unix/Linux Variant Systems

NOTE THAT THE TERM "SENIOR ADMINISTRATOR" IS DEFINED AS A DEAN, VICE-PROVOST OR VICE CHANCELLOR OR DESIGNEE (Source Cyber-safety Policy, PPM310-022)
YOUR RESPONSES TO EACH QUESTION SHOULD REFLECT THE OVERALL LEVEL OF CYBER-SAFETY COMPLIANCE. IN THE EVENT THAT SPECIFIC SYSTEMS OR VLANS DO NOT MEET THE OVERALL LEVEL OF COMPLIANCE, PLEASE DESCRIBE THE DISCREPANCIES IN YOUR RESPONSE TO THE FINAL "ADDITIONAL INFORMATION" QUESTION IN THE APPLICABLE SECTION.
SECTION 1: INSECURE PERSONAL INFORMATION

Campus units must identify departmental computing systems and applications that store personal information (personal name along with Social Security number, California driver identification number, financial account information, health insurance information or medical account information). Personal information must be removed from all computers for which it is not required. If the personal information cannot be removed from the computing system, the campus unit must develop a plan specifically outlining how the information and systems will be kept secure. Measures to protect the information could include removing several digits from the personal identifiers, moving the files to removable media and storing this media in a secure location apart from the computer, or encrypting the personal information. Campus units providing electronic personal information, as defined above, to another party must do so by a formal agreement. The agreement must include a provision that replicates this data standard for the party receiving the electronic personal information.

Campus units that develop network-based applications that host personal information must use secure application coding practices (see Web Application Security Standard within Level 2 Security Practices).

1. Have you completed a process to identify systems and applications within your unit that store personal information?
   a. Yes
   b. No (skip to 1.6)

2. Do you use an automated search tool to identify personal information residing in desktop and laptop computers?
   a. Yes
   b. No (skip to 1.6)

3. Describe the scanning frequency for personal identity information. At least:
   a. Weekly
   b. Once per month
   c. Bi-monthly
   d. Once per quarter
   e. Once per year
   f. Irregular frequency

4. What automated tool is used for this search function?

5. Please indicate which devices are subject to this search?
   a. Desktops
   b. Laptops
   c. Servers
   d. Portable Electronic Data Media
   e. Not applicable

6. Do you have an automated tool to search databases for personal identity information?
   a. Yes
   b. No (skip to 1.8)

7. Please describe the database search tool(s)

8. Do you have a process to verify that personal information has been removed from electronic storage on systems where it is not required?
   a. Yes
   b. No (skip to 1.10)
9. Please describe the verification process.

10. If you store personal identity information on your computing systems and/or data storage devices, which of the following measures have been deployed?
   a. Whole disk encryption or portable media encryption (skip to 1.11)
   b. File encryption (skip to 1.11)
   c. Physically secure portable data storage (skip to 1.11)
   d. Other
   e. Not applicable – no stored electronic identity information (skip to 1.11)

   A. If Other, please describe.

11. Have you obtained a management exception with senior administrator approval exempting system(s) and/or storage devices from measures to protect personal identity data?
   a. Yes
   b. No (skip to 1.12)
   c. Not applicable – no exception necessary (skip to 1.12)

   A. If Yes, please describe, including the identification of the approver.

12. If your unit has developed network-accessible applications hosting personal information, have the applications been evaluated for use of common vulnerabilities, including the OWASP top ten application security vulnerabilities?
   a. Yes
   b. No (skip to 1.14)
   c. Not applicable – no network-accessible applications with personal information (skip to 1.14)

13. Who performed the evaluation?
   a. Unit developers
   b. External unit
   c. Other

   A. If Other, please describe

14. Does your unit share personal identity data with third parties?
   a. Yes
   b. No (skip to 1.18)

15. Is this sharing of personal identity data with third parties conducted through a formal agreement with security requirements for the personal identity data?
   a. Yes
   b. No (skip to 1.17)

16. Which of the following does the agreement cover?
   a. Contractor safeguarding data
   b. Prohibit unauthorized use or disclosure
   c. Deletion at the end of contract term
   d. Contractor agrees to abide by UC Cyber-Safety Policy
   e. Contractor will report unauthorized disclosures or misuse of data
   f. Contractor agreement for internal audit of data handing practices
   g. Contractor assistance in litigation or administrative proceedings in the event of security incident involving personal data
   h. No assignable third-party rights
17. Have you obtained a management exception approved by a senior administrator reducing the need for the protection of personal identity data in third party agreements?
   a. Yes
   b. No (skip to 1.18)
   c. Not applicable – no exception necessary (skip to 1.18)

A. If Yes, please describe, including the identification of the approver.

18. Enter any additional information you would like to include in this report regarding your practices to secure personal information:
SECTION 2: FIREWALL SERVICES

Campus units must deploy and maintain both a network (VLAN) firewall and host-based firewall service for network-connected computers. The firewalls must be restrictively configured to deny all traffic unless expressly permitted.

A VLAN firewall is a system that implements security policy to control traffic between a VLAN and networks external to the VLAN. A VLAN firewall provides routing services and may also offer network address translation services.

1. How many VLANs does your campus unit manage?

2. How many of your VLANs have a VLAN-level firewall deployed?

3. Are all of your computing systems behind a VLAN firewall with ingress filtering to authorized hosts?
   a. Yes
   b. No (skip to 2.5)

4. Which of the following rules are present on your VLAN firewall with ingress filtering?
   a. Deny all inbound traffic unless specified
   b. Normalize traffic (remove fragmented packets)
   c. Allow Echo, Destination Unreachable, Time Exceeded from campus addresses
   d. Allow Web traffic
   e. Allow SSH traffic
   f. Allow SMTP traffic
   g. Allow secure POP/IMAP email authentication
   h. Allow NTP time synchronization
   i. Allow DNS traffic (if you host an internal DNS server)
   j. Other
   A. If Other, please describe.

5. Are you running egress filtering on all your VLAN firewalls?
   a. Yes
   b. No (skip to 2.7)

6. Which of the following rules are present on your VLAN firewall with egress filtering?
   a. Deny all outbound traffic unless specified
   b. Normalize traffic (remove fragmented packets)
   c. Allow Echo, Destination Unreachable, Time Exceeded to campus addresses
   d. Allow Web traffic
   e. Allow SSH traffic
   f. Allow SMTP traffic
   g. Allow secure POP/IMAP email authentication
   h. Allow NTP time synchronization
   i. Allow DNS traffic
   j. Other
   A. If Other, please describe.

7. How frequently are VLAN firewall rules reviewed and, if necessary, updated? At least:
   a. Weekly
   b. Once per month
   c. Bi-monthly
   d. Once per quarter
8. A. How many Windows systems use a host-based firewall service? (Run check against unit information system totals)
B. How many Mac systems use a host-based firewall service? (Run check against unit information system totals)
C. How many Unix/Linux systems use a host-based firewall service? (Run check against unit information system totals)

9. Generally describe the predominant configuration of host-based firewalls within your unit:
   a. Ingress rules only
   b. Egress rules only
   c. Ingress and egress rules are present
   d. Not applicable – no rules present (skip to 2.12)

10. For systems using a host-based firewall service, are you running rules appropriate for the role of the system?
    a. Yes, rules are system-specific
    b. Yes, custom rules
    c. No, the same rules are applied to all systems
    d. Not applicable – no rules present

11. How frequently are host-based firewall rules reviewed and, if necessary, updated? At least:
    a. Weekly
    b. Once per month
    c. Bi-monthly
    d. Once per quarter
    e. Once per year
    f. Irregular frequency

12. Have you obtained a VLAN firewall or host-based firewall-related exception approved by a senior administrator?
    a. Yes
    b. No (skip to 2.13)
    c. Not applicable – no exceptions necessary (skip to 2.13)

A. If Yes, please describe, including the identification of the approver.

13. Enter any additional information you would like to include in this report regarding your firewall practices:
SECTION 3: AUDIT LOGS

Campus units must develop and implement a policy defining the use, inspection and retention of audit logs. Audit log inspection may permit the identification of unauthorized access to sensitive electronic communication records. The use of audit logs should be extended to document activities such as account use and the network source of the login, incoming and outgoing network connections, file transfers and transactions.

1. Do you have a formal campus unit policy or practice requiring the identification of systems for which audit logs will be activated AND specifying the events to be included in these audit logs?
   a. Yes
   b. No (skip to 3.7)

2. Do you have a formal campus unit policy or practice defining the frequency at which required audit logs are to be inspected?
   a. Yes
   b. No

3. Are your system audit logs inspected according to the frequency defined by policy or practice?
   a. Always
   b. At least 80 percent of the time
   c. Inconsistent compliance

4. Do you have a formal campus unit policy or practice defining the retention requirement for all required audit logs?
   a. Yes
   b. No (skip to 3.6)

5. Are the audit logs retained according to the retention policy or practice?
   a. Yes
   b. No

6. Describe how you secure your audit logs from unauthorized modification:

7. Have you obtained a management exception approved by a senior administrator that permits campus unit systems and/or devices to be without a formal policy or practice defining log use, inspection and retention?
   a. Yes
   b. No (skip to 3.8)
   c. Not applicable – no exception necessary (skip to 3.8)

A. If Yes, please describe, including the identification of the approver.

8. Enter any additional information you would like to include in this report regarding your campus unit audit log policy or practices.
SECTION 4: WEB APPLICATION SECURITY VULNERABILITIES

Web applications developed or acquired by campus units must support secure coding practices. Web applications must mitigate the vulnerabilities described within the OWASP Top Ten Critical Web Application Security Vulnerabilities.

1. Does your unit host Web applications or have contracts with a non-University provider to host any Web applications?
   a. Yes
   b. No (skip to 4.10)

2. Do any of your unit hosted Web applications or non-University provider hosting any Web applications contain or provide access to restricted information (e.g., information protected by law and/or policy – such as personal identity data or non-directory student information)?
   a. Yes
   b. No (skip to 4.10)

3. Describe the name or function each of the Web application(s) identified above.

4. Indicate which of the following Web application vulnerabilities for which your Web application is tested:
   a. Cross-site scripting
   b. Injection flaws
   c. Malicious remote file execution
   d. Insecure direct object reference
   e. Cross-site request forgery
   f. Broken authentication
   g. Insecure cryptographic storage
   h. Insecure communications
   i. URL access restrictions
   j. Please describe any other vulnerabilities for which you test:

5. Describe how you or your vendor tests your applications for any of the vulnerabilities you identified in 4.3:

6. Does your campus unit possess development, test and production servers for your Web application?
   a. Yes
   b. No (skip to 4.8)

7. Enter which of the following instances of your Web application are tested for the vulnerabilities you identified in 4.3:
   a. Development
   b. Test
   c. Production

8. Describe how you ensure development staff are knowledgeable of secure coding practices for Web applications.

9. Have you obtained a management exception approved by a senior administrator that exempts your campus unit from developing/using Web applications that employ secure coding practices?
   a. Yes
   b. No (skip to 4.10)
   c. Not applicable – no exception necessary (skip to 4.10)

A. If Yes, please describe, including the identification of the approver.

10. Enter any additional information you would like to include in this report regarding your approach to identity and eliminate Web application security vulnerabilities?
SECTION 5: VULNERABILITY SCANNING PARTICIPATION

1. Do you permit the campus vulnerability scanners (169.237.224.0/26) to communicate to your all systems residing on each of your unit VLANs?
   a. Yes (skip to 5.6)
   b. No

2. Provide the VLAN addresses and names that are bypassing the scanners.

3. Describe each of the system(s) and the reasons for excluding the unit system(s) from the scans or enter ‘not applicable’

4. For those VLANs not opened to the campus vulnerability scanners, please describe:
   a. VLAN(s) has/have no network equipment
   b. VLAN has an exception from scanning that has been authorized by my Dean, Vice-Chancellor, Vice Provost or other senior campus administrator
   c. Not applicable

5. Enter any additional information you would like to include in this report regarding your approach to vulnerability scanning?