Risk Analysis for Financial Banking and Processing

Training Cybersecurity Workforce through Academia and Industry Collaboration

Moderator:
Dr. Paul Wang, Professor CSU

Panelists:
Dr. Wayne Summers, Professor, Chair CSU
Michael Barker, C-4
Kendrick Golston, Student CSU

Session B-4, Monday 11/7, Time: 2:15PM – 3:00PM
Vulnerabilities in Financial Banking Industries

- 7,111 financial institutions analyzed for vulnerabilities in 2016
  - Investment banks
  - Asset management forms
  - Major commercial banks
- 75% out of the top 20 US banks are infected with malware
- 95% out of the top 20 US banks have a network security grade of “C” or below
- Only one of the top 10 banks received an overall “A”

Source: PWC’s Global Economic Crime Survey
Non-compliant PCI responses by finance companies

- PCI 1 Issue types associated with authentication for use of the technology [general information security]
- PCI 3 Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

Source: SecurityScorecard
The gap...

Cybersecurity education does not cover financial sector KSAs

Financial major programs does not provide advanced security training
To close the gap…

Cybersecurity workforce development + Financial banking and processing security
Academia and Industry Collaboration

– TSYS needed mainframe programmers (1990s)
  ➔ ICAPP (10 course / 2 semester)
– TSYS / AFLAC needed PEGA Developers (2015)
  ➔ PEGA Certification (2 course / 2 semester)
– OmegaFi needed software developers, database analysts, …
  ➔ 20/25 IT employees are CSU grads
– TSYS (and everyone else) needs Cybersecurity Professionals
Academia and Industry Collaboration

♦ TSYS’s recent gift $4.5 million to Computer Science
  – ($2.5 mill for cybersecurity)
    • TSYS Center for Cybersecurity
    • Faculty Professional Development
    • Outreach Activities
Building a Center for Cybersecurity

♦ Mission
♦ Learning Spaces
♦ Function
♦ Next Steps
Building a Center for Cybersecurity
TSYS Center for Cybersecurity
TSYS Center for Cybersecurity

- K-12 Industry Day

Rothschild Academy Cybersecurity
Academia and Industry Collaboration

- Synovus Banking
  - Providing Real World problems

- OmegaFi
  - awarded four (4) $5K scholarships for CSU students
    - Linked with internship working as a team
  - Real World Problem
Academia and Industry Collaboration

A. Student needed to replace a required course
   WBIT 4602. IT Seminar

B. Local company need for risk analysis in financial processing
   (PCI/DSS compliance)

C. Created Independent Study class with Dr. Wang as the SME
Michael Marker, C-4

- Shortage of cybersecurity workforce
- Private sector and academia collaboration
- Risk analysis for banking industry
- NICE framework guide cybersecurity training
- Importance of student internship
Study Process & School Experience

*Kendrick Gholston, CSU Student*

- CSU recommends that a student spends at least 15 hours a week outside of school programming.
- My study process is that I do the recommended time a week while also spending about 6 hours a day studying through the use of detailed notes and recordings to fully understand the concepts.
- Part of the student organization Black Box Society which is devoted to all things related to computer security, cybersecurity, and information security.
- Competed in two cybersecurity competitions including the Ghost Red CTF and the Southeastern Collegiate Cyber Defense Competition.
Internships

• Aflac
  – Took part in their summer internship program
  – Learned from Aflac executives through their Leadership Engagement series
• OmegaFi
  – Very unique internship as this is the first time OmegaFi has awarded an internship to those who won their scholarship
  – Role is that of a Web Application Developer Intern
  – Part of a collaborative group of 4 to work on an application called Security Manager.
  – Our goal from August to December is to improve Security Manager as to give a more ease of use.
Security Manager

- Security Manager is an application that is used to grant certain rights/permissions to and within OmegaFi applications.
- The current production build of it is riddled with user criticism with it feeling very outdated and disjointed.
- We wanted to give the application a more modern feel as well as improving the current functionality.
- Upon gathering the business requirement documents, we noticed 3 consistent changes that employees wanted to see.
Objectives for Security Manager

• Data Integrity
  – Currently the application draws employee data from two different databases, but in one database we noticed inconsistent data compared to the other.
  – Our goal is to move away from using both and only draw from database as to keep the data accurate.

• Principle of Least Privilege
  – In the current build, administrators for any application can grant permissions to applications that are not essential for their function
  – We are working to make a hierarchy of users: User- Basic access to whatever applications they use, General Admins– Grants permissions to their respective application, and “Super” Admins- Grants permissions to any application

• UI/UX
  – Incorporated elements of CSS and Bootstrap to give it a modern feel similar to OmegaFi’s other applications.
Reflections

• Real word application of what I’ve learned from school and the challenges of that application
• Starting to realize the synergy between schools and companies working closely together
• Look at this year as one that truly showed how prepared my courses have made me for my career endeavor
DevOps to DevSecOps

- Build it faster
- Protect it
- Keep it stable

Development

Security

Operations
Agile Methodology

- **Waterfall**: larger effort, High risk
- **Agile**: small effort, Low risk
Security as Compliance

- OmegaFi Information Security Policy
  - PCI DSS v3.1 (2016)

- PCI-DSS v3.2 (from v.3.1)

- ISO 13569
  - Financial services -- Information security guidelines (2005)

- ISO 27001
  - Information technology — Security techniques — Information security management systems — Requirements (2013)
**PCI-DSS v3.2**

**Goals and Requirements (left) | Requirement, Objective, Test Procedure, and Guidance (right)**

---

**PCI Data Security Standard – High Level Overview**

| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data  
| 2. Do not use vendor-supplied defaults for system passwords and other security parameters  
| Protect Cardholder Data | 3. Protect stored cardholder data  
| 4. Encrypt transmission of cardholder data across open, public networks  
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update anti-virus software or programs  
| 6. Develop and maintain secure systems and applications  
| Implement Strong Access Control Measures | 7. Restrict access to cardholder data by business need to know  
| 8. Identify and authenticate access to system components  
| 9. Restrict physical access to cardholder data  
| Regularly Monitor and Test Networks | 10. Track and monitor all access to network resources and cardholder data  
| 11. Regularly test security systems and processes  
| Maintain an Information Security Policy | 12. Maintain a policy that addresses information security for all personnel  

---

**Build and Maintain a Secure Network and Systems**

**Requirement 1:** Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity’s networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity’s internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity’s trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

**PCI DSS Requirements**

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Testing Procedures</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Establish and implement firewall and router configuration standards that include the following:</td>
<td>1.1.1 Establish and implement firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:</td>
<td>Firewalls and routers are key components of the architecture that controls entity to and exit from the network. These devices are software or hardware devices that block unauthorized access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization’s first line of defense in the protection of its data remain strong.</td>
</tr>
<tr>
<td>1.1.1.a For a sample of network connections, interview responsible personnel and examine records to verify that firewall configurations were approved and tested.</td>
<td>1.1.1.2 For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested.</td>
<td>A documented and implemented process for approving and testing all connections and changes to the firewall and router configurations. If changes are not approved, and not recorded, like this, unauthorized changes could lead to inconsistencies between network documentation and the actual configuration.</td>
</tr>
</tbody>
</table>
Duplications

7.1.1.0.00  7.1.1.0.0  Define access needs for each role, including system components and data resources. In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role.

7.1.2.0.00  7.1.2.0.0  Restrict access to privileged users/IDs to least privilege necessary to perform job function. When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the “least privilege”).

7.1.3.0.00  7.1.3.0.0  Assign access basing individual personnel’s job classification and function. Once needs are defined for user roles [per PCI DSS Requirement 7.1.1], it is easy to grant individual access according to their job classification and function.

7.1.4.0.00  7.1.4.0.0  Document approval by authorized personnel specifying required privileges. 7.1.4.0 Document approval, for example, in writing pre-technically assures those that with access and privileges are known and authorized by management.

7.1.6.0.00  7.1.6.0.0  Establish an access control system(s) for system components that restricts access based on a multifactor authentication method. Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access.

7.2.1.0.00  7.2.1.0.0  Coverage of all system components. Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access.

7.2.2.0.00  7.2.2.0.0  Assignment of privileges to individuals based on job classification and function. Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access.

7.3.0.0.00  7.3.0.0.0  Default “deny” setting. Without a mechanism to restrict access based on user’s need to know, a user may unknowingly be granted access.

7.3.0.0.0  7.3.0.0  Ensure that security policies and operational procedures for restricting access to cardholder Personal need to be aware of and followed. Security policies and operational procedures to ensure that access is controlled and based on need.

8.1.0.0.00  8.1.0.0.0  Define and implement policies and procedures to ensure proper user identification, authorization, authentication, and access control. By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization may be able to know who has access to what information.

8.1.1.0.00  8.1.1.0.0  Assign all users a unique identifier allowing them to access system components or cardholder data. By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization may be able to know who has access to what information.

8.1.2.0.00  8.1.2.0.0  Control addition, deletion, and modification of user IDs, credentials, and other identifiers. To ensure that user accounts granted access to systems are all valid and recognized users. Strong processes must manage all changes to user IDs.

8.1.3.0.00  8.1.3.0.0  Immediately revoke access for any terminated user. If an employee has left the company and still has access to the network via their user account, unauthorized or malicious access to cardholder data may occur.

8.1.4.0.00  8.1.4.0  Remove/delete inactive user accounts within 90 days. Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed.

8.1.5.0.00  8.1.5.0  Manage IDs used by third party access support, or maintain system components via a Service Level Agreement for 24/7 access. By having a SLA in place, an attacker can attempt to guess passwords through manual or automated tools.

8.1.6.0.00  8.1.6.0  Limit repeated access attempts to lockout the user ID after no more than six attempts. Without account-lockout mechanisms in place, an attacker can attempt to guess passwords through manual or automated tools.

8.1.7.0.00  8.1.7.0  Limit password expiration to a minimum of 30 minutes or until the administrator enables the lockout. If an account is locked out, it’s mission-critical to avoid reusing the locked account.

8.1.8.0.00  8.1.8.0  If a session has been idle for more than 15 minutes, require the user to reauthenticate. When users walk away from their system or lock their machines, that machine may be used by other attackers.

8.2.0.0.00  8.2.0.0  In addition, assign a unique ID, ensure proper user authentication and management. For these authentication methods, when used in addition to unique IDs, help protect users/IDs from being compromised, since the one thing attackers can’t do is create multiple users/IDs.

8.2.1.0.00  8.2.1.0  Using strong cryptography, rotate user authentication credentials such as passwords. Many network devices and applications transmit unencrypted, readable passwords across the network and for storage purposes without encryption.

8.2.2.0.00  8.2.2.0  Verify user identity before modifying any authentication credentials—for example, perform a biometric scan. Many malicious individuals use “social engineering” for example, calling a help desk acting as a legitimate user to have a password reset.

8.2.3.0.00  8.2.3.0  Passwords/passphrases must meet the following 8 B. A minimum length of at least 8 characters, must contain a mix of letters, numbers, and symbols, and should not be a common password.

8.2.4.0.00  8.2.4.0  Change user passwords/passphrases at least once every 30 days. Passwords/passphrases that are valid for a long time without change provide malicious individuals with more time to work the password.

8.2.5.0.00  8.2.5.0  Do not allow an individual to assume a new password/passphrase that is the same as any old password history isn’t maintained, the effectiveness of changing passwords is reduced, and passwords can be reused over and over again.

8.2.6.0.00  8.2.6.0  Set passwords/passphrases for first time users and upon request to at least 8 characters for each user. If a new password is used for every new user, an attacker may discover the password.

8.3.0.0.00  8.3.0.0  Secure all individual non-cardholder administrative access and remote access to the CDE. Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication (as required in Requirement 8.3.1.0).

8.3.1.0.00  8.3.1.0  Incorporate multi-factor authentication for all non-cardholder CDE access for personnel. This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access to the CDE.

8.3.2.0.00  8.3.2.0  Incorporate multi-factor authentication for all remote access systems (both users and administrators) to apply to all personnel—administrators, and users (for support or maintenance) within the organization.

8.3.3.0.00  8.3.3.0  Document and communicate policies and procedures to all users including Communicating password/authentication policies and procedures to all users helps ensure that users understand and abide by the policies. For example:

8.3.4.0.00  8.3.4.0  Do not use group, shared, or generic IDs, passwords, or other authentication methods as if multiple users shared the same authentication credentials (for example, user account and password). It becomes impossible to trace system access.
PCI-DSS v3.2
Architecture

- Goals (6)
- Objectives (12)
- Requirements (251)
- Procedures (412)
- Guidance (214)
PCI-DSS v3.2 Framework relationships
Close the Gap
viCyber - NSA CNAP CAE-C Grant

- Cloud-based repository of knowledge essential for cybersecurity training design according to nationally recognized frameworks
- A Visually Intelligent Tool for Rapid Cybersecurity Training/Curriculum Development
Take-away

• Risk analysis for financial sector
  – DevSecOps + Agile

• PCI-DSS databases
  – ISO, FISMA etc.

• NICE framework
  – Cybersecurity training and development - viCyber

Cybersecurity = Hardware + intelligence + Software + Policy + Operation (HiSPO)
Q&A