Access Control & User Authentication for Precision Contents Inc.
Team/Student Name(s): Karl Colimon/Enrique Mertins | Business Advisor Name: Rick Belmont | Professor: Dr. Yair Levy

Introduction

Retail store Crystal Connections currently does not have a formal inventory or point of sales system (PoS). In an effort to modernize the process and address issues with ‘shrinkage’ the company has enlisted the services of Precision Content a company specializing in inventory management and small business solutions. Precision content is overseeing the development of a Point of Sale system (PoS) with an integrated inventory management system. Security will be the central focus of the system install. An article by pcmag.com points out that PoS intrusions account for 33% of all data breaches (Rashid, 2014) The point of contact for this project is Rick Belmont founder and president of Precision Contents Inc.

Project Scope, Goals, and Objectives

Project Scope:
- Evaluate the accuracy of physical and system controls of Crystal Connections Inc. as well as evaluate the security vulnerabilities of the cloud based Point of Sale (PoS) system implemented by Precision content Inc.

Goals and Objectives:
- Operational Objectives: The project will evaluate the data integrity, confidentiality of customer data, access controls, system availability, and Infrastructure.
- Control Activities: Evaluate that appropriate authority is established in the system; for example, managers have to authorize returns and reprising of items.
- Reduce losses from shrinkage

Problem

Crystal connections lacks adequate controls over sensitive costumer and employee data; such as, credit card information, customer personal information, employee lack training on how to prevent fraud, and lack of oversight leaves the organization open to theft. In addition, there is a lack of proper inventory management leaving the business at risk of incurring losses from ‘shrinkage’. There is no mechanism for fraud detection.

Inventory Shrink

- Unknown Error 44%
- Vendor Error 34%
- Administration Error 15%
- Employee Theft 3%
- Shoplifting 4%

"The 2007 National Retail Security Survey put losses from inventory shrink at as much as $34.8 billion. Astoundingly, employee theft represented 44% of these losses, surpassing Shoplifting at 34%" (Digital Persona, 2009).

Possible Solutions and Plan

1. Separating conflicting responsibilities
2. Define the internal application security mechanisms that provide users with the specific functions necessary for them to perform their jobs
3. Asses the adequacy of preventive and/or detective controls
4. Separate incommunicable duties within an organization and provide the correct level of empowerment
5. Secure the host computer system where application systems and related data are stored and processed from

Risk Management Analysis Outline

<table>
<thead>
<tr>
<th>Risk Likelihood</th>
<th>Risk Source</th>
<th>Impact</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Integrity</td>
<td>Data corruption</td>
<td>Loss of data, possible duplications of information, or in some cases full loss of all files on the application.</td>
</tr>
<tr>
<td>Medium</td>
<td>Confidentiality /Timeliness and Relevance and Access</td>
<td>Inappropriate or inadequate security access controls</td>
<td>Confidentiality violation, data lost or data corruption by virus, worm, Trojan programs, or unauthorized users.</td>
</tr>
<tr>
<td>Medium</td>
<td>Confidentiality /Timeliness and Relevance and Access</td>
<td>Inappropriate or inadequate security access controls</td>
<td>Data lost or data corruption by virus, worm, Trojan programs, or unauthorized users.</td>
</tr>
<tr>
<td>Low</td>
<td>Availability</td>
<td>Natural disasters (Fire, Flood etc.) causing hardware and software failure. Power outage. Corruption. Etc.</td>
<td>Short term / Long term business disruption to system</td>
</tr>
<tr>
<td>Low</td>
<td>Infrastructure</td>
<td>Lack or weak execution</td>
<td>Disorganized and dysfunctional IT decisions. Lack of proactive security policies and procedures or inconsistent one among IS and divisions</td>
</tr>
</tbody>
</table>

Anticipated Results

1. Improve ability of management to detect fraudulent activity
2. Reduce financial loss due to shrinkage
3. Cost savings from fraud prevention
4. Shorten turnover time with customer orders

Proposed Cost

<table>
<thead>
<tr>
<th>Resource and Cost</th>
<th>Time Estimates per resource</th>
<th>Cost in US dollars</th>
</tr>
</thead>
<tbody>
<tr>
<td>Developers: $38/hr.</td>
<td>5 hours</td>
<td>$190</td>
</tr>
<tr>
<td>Trainer: $25/hr.</td>
<td>32 hours</td>
<td>$800</td>
</tr>
<tr>
<td>Auditor: $50/hr.</td>
<td>32 hours</td>
<td>$2,560</td>
</tr>
<tr>
<td>Project Manager: $37/hr.</td>
<td>40 hours</td>
<td>$1,480</td>
</tr>
<tr>
<td>Business Analyst: $25/hr.</td>
<td>40 hours</td>
<td>$1,000</td>
</tr>
<tr>
<td>Telesur: $30/hr.</td>
<td>40 hours</td>
<td>$1,280</td>
</tr>
<tr>
<td>Miscellaneous</td>
<td>+25%</td>
<td></td>
</tr>
<tr>
<td>Totals estimated cost:</td>
<td>$9,137</td>
<td></td>
</tr>
</tbody>
</table>

References

Constantin, L. (2014, 4,22). Web apps and point-of-sale systems were leading hacker targets in 2013, says Verisign. Retrieved 11 9, 2014, from PCWorld.com:


Conclusion

Due diligence must be paid when implementing Point of Sale Systems to assure that confidential information is secured. Preventative measures must be taken to identify potential risks. According to John Yeo Yeo EMMA Director at Trustwave “the average time it took companies to actually detect an intrusion from the time it occurred was 87 days” pcworld.com. The systems must be configured and proper controls in place to reduce the risk of unauthorized access and facilitate early detection. Segregation of duty is essential to assure that one person does not have sole access to all aspects of the payroll system, thus is unable to manipulate the data. Additionally, we recommend adapting a Chip and Pin system as stated by John Yeo EMEA Director at Trustwave states that EMV–chip and Pin payment card transactions have shifted the focus of criminals away from PoS systems to e-commerce pcworld.com 2014.

Graduate School of Computer and Information Sciences (GSCIS)

Center for Information Protection, Education, and Research (CIphER)