Security Audit

by

Kyle Bridges

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

4/22/14

Kyle Bridges

Date

4/22/14

Mark Stockman, Faculty Advisor

Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2014

Table of Contents

List of Figures

Abstract

What if there was a security issue on a company's network and someone else found it before the network administrators did? Imagine if someone was able to gain vital company information such as financials, or confidential employee files. To keep networks safe the solution to prevent this problem from happening is conducting annual security audits. By assessing all areas of security including physical, network, and application the risk of exposure can be reduced greatly. By assessing known security issues more potential security breaches were found along the way. Solutions were created and put into place to resolve potential security risks. These risks included separated employees having access to systems for a period after they were separated, badge system server being out of date possibly making the security badge system nonfunctional any longer, and creating training on IT security for employees. A SharePoint process was put into place to resolve this problem. By upgrading the physical badge system server, new versions of the software were able to be installed and provided more secure features as well as managing all building locations from one place. The risk of the server crashing and access control not functioning has been reduced and security to the building has increased. Employee training on security best practices made the employees aware of potential risks to their own accounts due to their actions. The training resulted in fewer account related issues by the users reported to the help desk. The results of this project mean a more secure environment for the company and its users. By putting these solutions into place the company can save time, money, and have increased positive awareness of security and the role it plays in the workplace.

Introduction

In this senior project there were multiple problems addressed. There was a SharePoint solution that was put into place to help retain company information such as customer, and carrier data. The possibility of separated employees retaining access to their past emails and customers could result in a major loss to the company in the future. Depending on the amount of data that could possibly be exposed the company could possibly have losses of business in the millions. The goal of this project is to increase data security not only on a software level but physically as well. Another part of this project involves an upgrade to the current badge readers and to the software that controls these access points. The upgrade will be from ProWatch to WinDSX. With the upgrade to this software the company can virtualize the server as well as remote a dated physical box that is no longer reliable. The software is able to support all satellite offices and the headquarters which are spread all over the country in one centralized place of management.

Problem

The main problem is that there are many minor security flaws in the current network that could become huge problems for the company. These flaws could potentially allow company clients'/customers' information to be released to the whole company or even outside the company. There are problems in multiple layers of security including physical, network, and application. Employee badges are not being exercised or used properly as many people can enter the building with one person scanning their badge to open the doors. Also the employee termination/separation process is flawed. Separations take place and the notices are not sent in until later in the day or even sometimes the next day. This is important because users could still access their accounts and retain valuable company information before their access is cut. There are several questions to be answered. For example how do we get employees to exercise the badging system properly? How do we keep client/customer information inside the system and not allow for it to get out to the public? What process can we use to cut separated employees access to the company's systems as soon as they are separated? And finally how do we do all of this without making the employees feel uncomfortable and keeping users productive?

The other major problem that is being addressed in this project is the badge system and upgrading the server and getting all offices on the same program. Right now all of the 22 satellite offices are on a different product than the Cincinnati headquarters and the other Cincinnati locations. The current system is hosted on an aging physical server box and needs constant maintenance to keep it alive and running. The constant maintenance of this server is costing the company extra money and taking up time the network administrators could be using to do more important projects.

Solution

Company security against separated employees is very important. If an employee is separated from the company and is possibly angry they could cause a lot of trouble for the company. For example, in the past there have been issues with employees still having access to their user accounts and emails for some time after they are actually separated in the system. This could possibly allow for past employees to still have access to their customer information and possibly use it in the future for their own good and take business away from the company. In order to combat this possibility there has been a

SharePoint solution put into place to solve the issue of employee terminations. There is now a form that the manager of the employee fills out and it gets sent right to HR. Once HR finalizes the form it is submitted to IT and the connections to the users Active Directory account and exchange account are automatically disabled. This is a real time solution and has been working out great the past couple months.

In terms of physical security the building has a strong foundation to be secure. Most of the risk involved comes from actual employees. For example, one user might badge in the door and allow the next five people in after they pass. The unregistered entrance of these extra employees without record is a security risk. Also, TQL has many satellite offices across the country and they use different software for the badging system than the headquarters. In order to get all of the locations on the same software I will be creating a new virtual server and updating the building hardware and software to resolve this issue. This will then create a single point of failure and only one point of the network to maintain. The specifics on the design and implementation of these solutions will be explained later in this report.

Project Goals

My project goals include implementing a SharePoint solution to help with the employee separation problem, upgrading the badging system server, and upgrading the Milford Ohio location as well as the Ivy Pointe locations to DSX from ProWatch. My final goal is once the entire company and all of its locations are on DSX to add in a driver that will allow for the security cameras to be integrated as well. The remainder of this final report outlines in detail how the project was completed. The report includes the following sections: design objectives, methodology, budget, timeline, problems encountered, and future recommendations.

Project Concept

This project came to my attention when the Director of IT at TQL approached me with a list of projects that needed to be looked at but there was currently no extra time to explore them. I chose off of the list the topics that interested me the most, information and physical security.

Design Objectives

The goals of this project were one, to decrease the risk of terminated employees of gaining access to their customer's information for personal use, and two, to upgrade the badge system server and at the same time upgrading the Cincinnati Ohio headquarters with new door hardware and upgrade to DSX. The solution for the risk of customer information getting out would be one that would have to be quick and immediate. The design and implementation of this part of the project will be discussed later in this report. The DSX upgrade came to be due to the need of a system and software that was able to easily manage an enterprise company with many locations around the country in real time, and at the same time. The system was chosen due to its' ability to manage all twenty-two of TQL's satellite offices and other major benefits that will also be discussed later on in this report.

Background on SharePoint and WinDSX

In order to help better understand my project and the solutions that were implemented here is some background on SharePoint and WinDSX. SharePoint is a web application platform developed by Microsoft in 2001. SharePoint is comprised of a set of web technologies build to work with other Microsoft products to create business solutions. According to Microsoft, SharePoint is used by 78% of Fortune 500 companies (Microsoft Corporation). DSX access systems is the company that created WinDSX as an access control program. They are based in Dallas, Texas and design all of their hardware and software in house. Also DSX integrates solutions with real world applications.

Data Center Core Diagram

The diagram below shows the data center core of the TQL network. The data center is comprised of many terminal servers that are used by remote satellite office users through a remote desktop session. The server being upgraded for DSX is located in the data center on a virtual server. The data center as TQL is top of the line and has an uptime of 99.999.

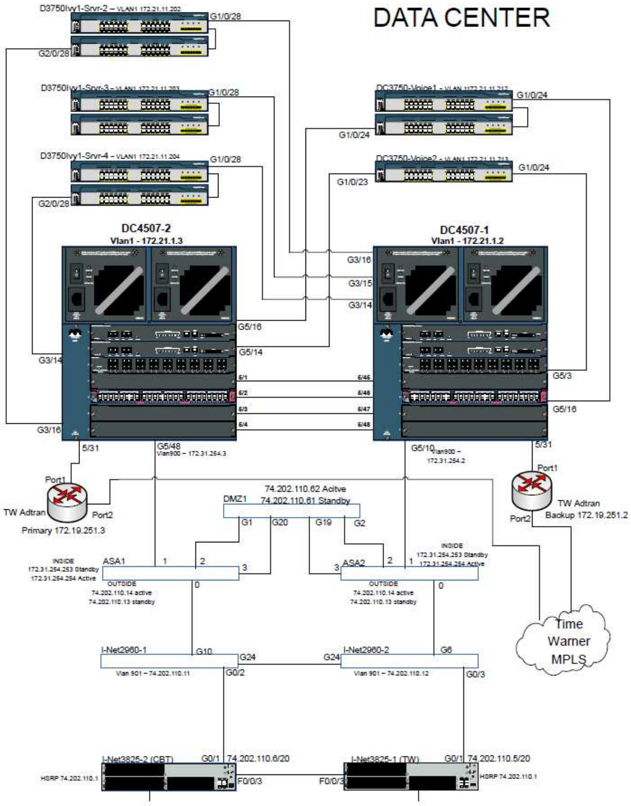


Figure 1

Methodology/Technical Approach/Technical Elements

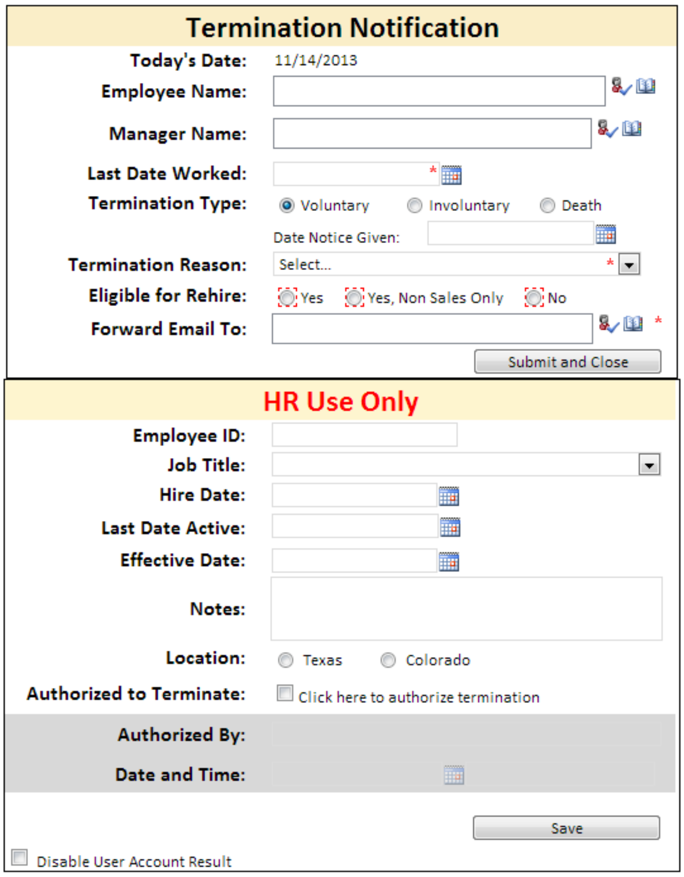
The requirement for this project was to use SharePoint to create a solution for the employee separation project and also to upgrade the headquarters to the DSX software. TQL runs an enterprise level Microsoft environment. Over the past few years the company really has been using SharePoint to create many solutions and workflows. Many departments within the company use SharePoint so it was only natural to try to tackle the employee separation problem with a SharePoint solution. This solution uses many programs including Active Directory, SharePoint, and Exchange. The process for this solution will be shown later in this report.

There are many technical aspects used in the DSX upgrade. This solution includes software tools such as, hyper v, WinDSX for SQL server, access, and Prowatch. Hardware elements of this project include new door lock mechanisms, and new controllers in the building. The building was built in 2007 and the door badge readers are currently outdated Honeywell readers. The system currently in use for this building location is called Prowatch. The reason for the upgrade to DSX from Prowatch is that as the company expands and adds more and more offices the software cannot support multiple locations very easily. WinDSX can handle as many offices as there are licenses for and can integrate all of these locations into one central management location.

Procedures

In order to tackle the problem of company information possibly going outside of the company by separated employees; the main ways they could do this had to be identified. Sales employees have access to two main information streams to achieve this goal if desired. They have the TQL Load Manager, which is the program that holds all of the customer, carrier, and load information, as well as their outlook email accounts. The way that separations worked at the time is as follows. Sometime during the day a manager would separate an employee, the manager would then contact the human resources department to begin the separation process. The IT helpdesk would not be notified of this until the end of the day normally around five p.m. Then one member of the IT helpdesk would manually by hand disable Active Directory accounts. Then exchange accounts as well as wipe the employees' cell phones to factory defaults if they had email on their phones. This is where the problem then occurs. For example, say John Doe is separated from the company at ten a.m., that same day they have roughly seven hours to go through their past and current emails. Then at that time they go through and find out and possibly save all of their customer information. By the time five p.m. comes around and the accounts are disabled the amount of information that was stolen could result in millions of dollars in possible lost future sales. This was the problem with the model of delayed separations being processed.

In order to combat this problem and prevent this issue from possibly happening in the future, a SharePoint solution has been put into place. This solution is very easy to use for all users and allows for automatic disabling of the Active Directory account, which will not allow the users to access their accounts and information. The solution is a SharePoint form as seen in figure 2 below.



Termination Notification

Today's Date: 11/14/2013

Employee Name:

Manager Name:

Last Date Worked: *

Termination Type: ● Voluntary ○ Involuntary ○ Death

Date Notice Given:

Termination Reason: Select... *

Eligible for Rehire: ○ Yes ○ Yes, Non Sales Only ○ No

Forward Email To: *

HR Use Only

Employee ID:

Job Title:

Hire Date:

Last Date Active:

Effective Date:

Notes:

Location: ○ Texas ○ Colorado

Authorized to Terminate: □ Click here to authorize termination

Authorized By:

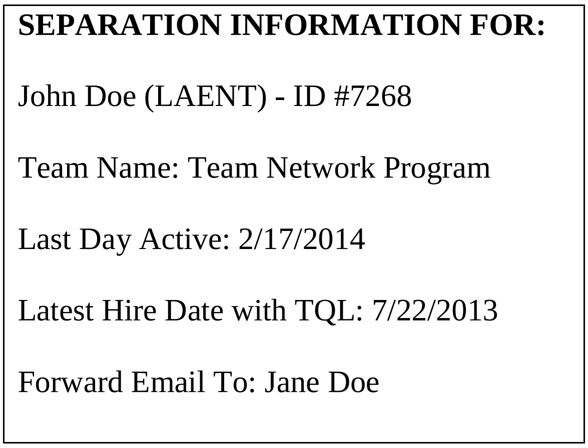
Date and Time:

□ Disable User Account Result

Figure 2

The top part of this form is specifically for the separating manager. The manager of the employee would simply fill in the employee name, their name, last date worked, type of termination, reason for termination, if they are eligible for rehire, and who to forward their email to so that the company does not lose any business due to this loss. The information entered in this form will help the recruiting department in terms of if they can rehire this employee in the future possibly in a different role. The most important part of the top section is who the users email is getting forwarded to. Typically this will be forwarded to another broker on the team who already knows what is going on with the specific customer.

The second part of this form which is on the bottom half is for the human resources department to utilize. Here information about the employee is entered into the system including, employee ID, job title, hire date, last active date, effective date, any notes needed for the system, office location, and the final authorization, along with the HR representatives name and time. With all of that information entered the box at the bottom left is checked and once the form is saved the Active Directory account for the user will automatically be disabled through a script. Once this form is complete an email is also generated to the IT helpdesk to confirm the separation. The generated email is in the format of figure 3 below.



SEPARATION INFORMATION FOR:

John Doe (LAENT) - ID #7268

Team Name: Team Network Program

Last Day Active: 2/17/2014

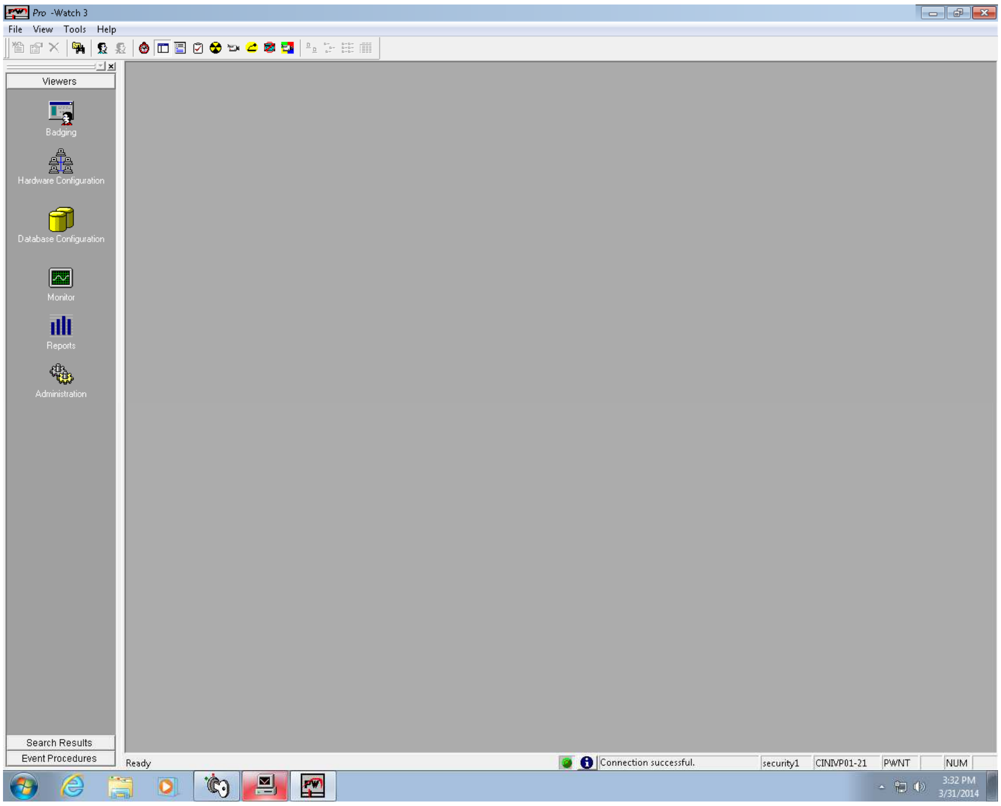
Latest Hire Date with TQL: 7/22/2013

Forward Email To: Jane Doe

Figure 3

In order to tackle the DSX upgrade many steps are needed to be completed to implement the solution. The first problem was the failing of the Prowatch server at the Ivy Pointe location. This is an old physical server from 2005 and the cost of keeping the system running was getting very high. The solution to this was to implement a virtual server in the Hyper V environment that could handle the amount of information being processed through the system. A system was then created with six cores, and six gb of memory to handle the possible add ins available in the future. The upgraded ram will allow for the install of an add in that can incorporate the security cameras into the DSX security monitoring system. The add in will allow for a camera to be turned on and record as soon as someone badges into the door located nearest to the camera. This way the system does not have to run 24/7 but only when it detects activity. In turn, this will save on storage space and allow for recordings to be saved for a longer period of time.

The main reason TQL is upgrading to WinDSX from Prowatch is that Prowatch does not do a good job of managing multiple office locations at the same time. With twenty two satellite office locations this software will not work for TQL and its' rapidly growing infrastructure. The figure below is a screen from Prowatch to show how dated the software is, and how there is no option for multiple office locations to be monitored.

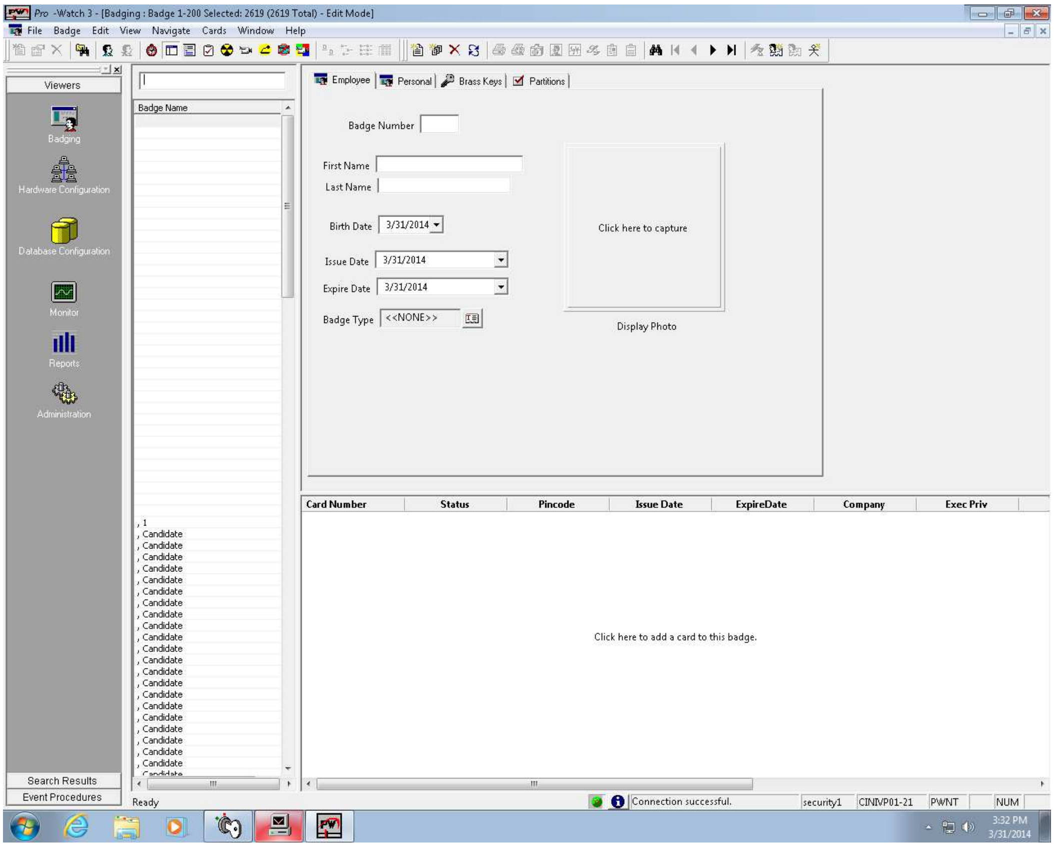


Connection successful.

security1 | CINIVP01-21 | PWNT | NUM

Figure 4

The main benefit of the Prowatch system currently is only the fact that there is a built in application for the employee security badge creation as seen below in Figure 5.



Pro -Watch 3 - [Badging : Badge 1-200 Selected: 2619 (2619 Total) - Edit Mode]

Badge Name

, 1
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate
, Candidate

Badge Number

First Name

Last Name

Birth Date 3/31/2014

Issue Date 3/31/2014

Expire Date 3/31/2014

Badge Type <<NONE>>

Click here to capture

Display Photo

Card Number	Status	Pincode	Issue Date	ExpireDate	Company	Exec Priv

Click here to add a card to this badge.

Ready

Connection successful. security1 CINVP01-21 PWNT NUM

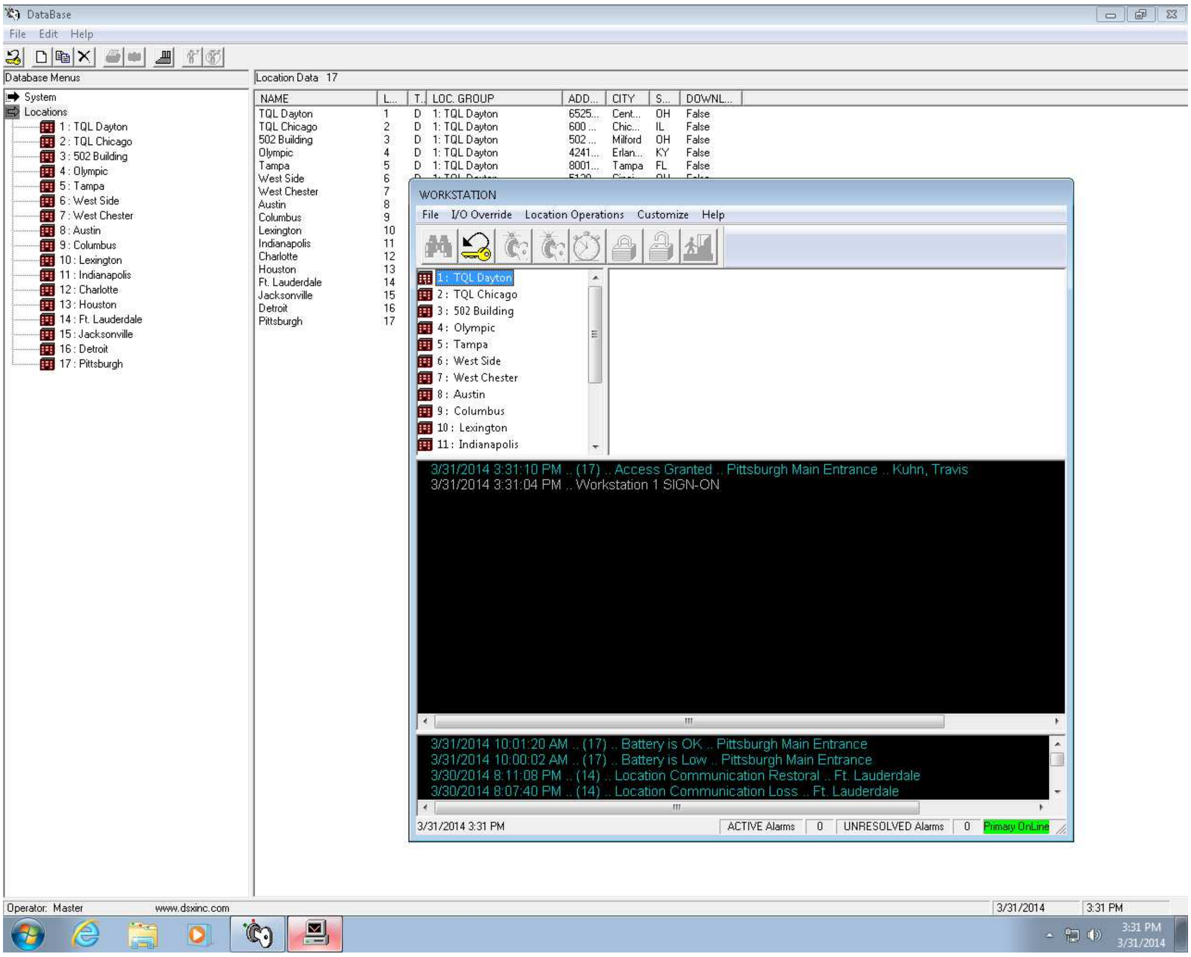
3:32 PM
3/31/2014

Figure 5

This feature however, will not be missed because there is an add in for a badge creator interface in WinDSX. WinDSX allows for many add ins that will make the software more functional and add to the all in one compatibility that is being created with the new software.

WinDSX offers many features that include but are not limited to: security camera integration, who is in report, time and attendance, elevator control, graphical maps, and graphical maps of the building with security points. The features listed make the software a great choice for a large and rapidly growing company such as TQL. Each satellite office was manually entered and configured separately at different times. However, all locations do show up on the same page and can be managed from one central location.

As mentioned earlier the main benefit of WinDSX is the ability to manage all office locations all over the country in one place. WinDSX also does live monitoring of all hardware components installed on all of the access points throughout all of the offices nationwide. The software also can provide detailed information such as who is entering which door, at which office, and at what time. The information can also be made into a report and sent off to anyone who may be requesting the information such as Executive staff members or managers. All of the information mentioned is displayed on the server in real time through a terminal window that shows all badging activity as well as the state of the hardware. Figure 6 below shows how the information is displayed.



Location Data 17

NAME	L...	T...	LOC. GROUP	ADD...	CITY	S...	DOWNL...
TQL Dayton	1	D	1: TQL Dayton	6525...	Cent...	OH	False
TQL Chicago	2	D	1: TQL Dayton	600 ...	Chic...	IL	False
502 Building	3	D	1: TQL Dayton	502 ...	Milford	OH	False
Olympic	4	D	1: TQL Dayton	4241...	Erlan...	KY	False
Tampa	5	D	1: TQL Dayton	8001...	Tampa	FL	False
West Side	6						
West Chester	7						
Austin	8						
Columbus	9						
Lexington	10						
Indianapolis	11						
Charlotte	12						
Houston	13						
Ft. Lauderdale	14						
Jacksonville	15						
Detroit	16						
Pittsburgh	17						

```
3/31/2014 3:31:10 PM .. (17) .. Access Granted .. Pittsburgh Main Entrance .. Kuhn, Travis
3/31/2014 3:31:04 PM .. Workstation 1 SIGN-ON
```

```
3/31/2014 10:01:20 AM .. (17) .. Battery is OK .. Pittsburgh Main Entrance
3/31/2014 10:00:02 AM .. (17) .. Battery is Low .. Pittsburgh Main Entrance
3/30/2014 8:11:08 PM .. (14) .. Location Communication Restoral .. Ft. Lauderdale
3/30/2014 8:07:40 PM .. (14) .. Location Communication Loss .. Ft. Lauderdale
```

3/31/2014 3:31 PM | ACTIVE Alarms 0 | UNRESOLVED Alarms 0 | Primary OnLine

Operator: Master | www.dsxinc.com | 3/31/2014 | 3:31 PM

3:31 PM 3/31/2014

Figure 6

In the figure above the information is displayed in the terminal window, an employee badged into the Pittsburgh main entrance at 3:31 p.m. on 3/31/2014. Another key feature to note is that the software actively communicates with all of the hardware within its network. For example, in Figure 6 the terminal window displays at the bottom that the battery is low at the Pittsburgh main entrance. The time, date, and error code are recorded in the logs for reference if needed in the future. When an error such as the ones mentioned occur the appropriate department such as building facilities is alerted. With this software all office locations will be physically secure 24/7/365.

Testing

The WinDSX software was first tested on the satellite office locations. Once those offices were successfully set up of the software in the Cincinnati area offices, they were able to be added without any problems. The switch over was in real time and flawless. No major issues were reported and there was no lapse in security during that time.

The WinDSX solution is very beneficial to TQL because the company now has one place to go to monitor office locations and get information such as badge reader times and access logs. The new server is able to handle the SQL version of WinDSX and is able to replace the dated physical Prowatch server. Having one central place to manage these systems reduces the risk of exposure due to one of the old three points of failure going down. The ease of use and management has gone up due to WinDSX, and the real time logs and monitoring of hardware has made all of the office location more secure. With the WinDSX implementation, all offices in the organization are on the same platform and this reduces time and work for the employee in charge of badge creation. This in turn, saves the company money down the road.

Budget

At the start of this project the company agreed to pick up the cost of the overhaul to the DSX security environment. In the figure below the cost was broken down by location and software costs. The cost of the SQL version of the WinDSX software was $2,208.52. The cost of the Ivy Pointe location and Edison locations totaled $21,839.35 for a grand project total of $25,671.10. The cost of this project was well worth the money due to the fact that a possible data leak for the company could cost it millions of dollars. A full detailed version of the budget can be found in Appendix A.

Description	Cost
Upgrade to SQL Version of DSX	$2208.52
Ivy Pointe Upgrade Hardware Takeover	$16,891.80
Edison DSX Takeover	$4,947.55
Total:	**$25,671.10**

Figure 7

Gantt Chart

The Gantt chart below helped the project stay on track and on time. The first part of the timeline was used mostly for research for the project. Once January hit and the project was ramping up in full swing, weekly goals were added and achieved on time. The project did not have any delays and was completed according to plan. (See Figure 8).

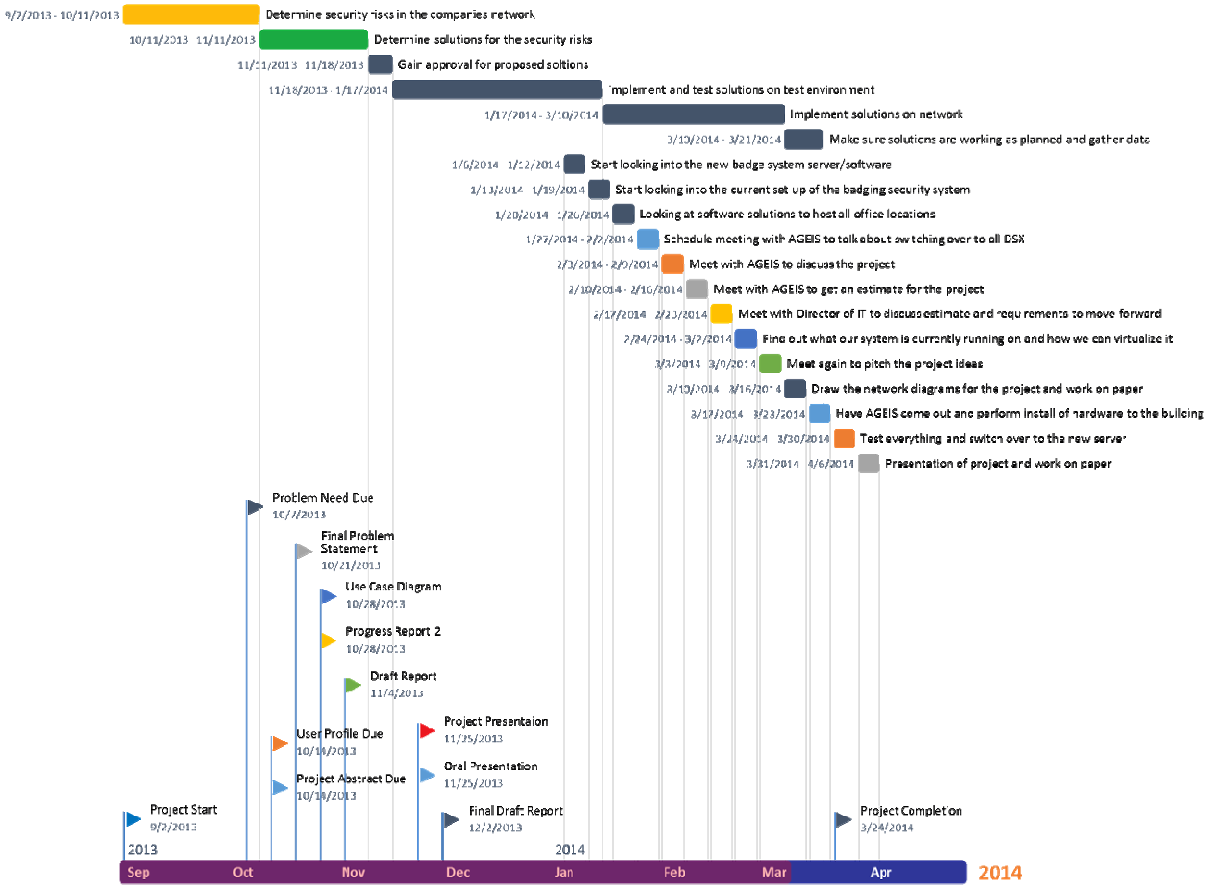


Figure 8

Use Case Diagram

For this project there are many users and departments that will be using the solutions that are put into place. The use case diagram below (Figure 9) shows that the IT administrators are in charge of maintaining and auditing the network. On the other side of the diagram the user is shown using the network at the same time while the admins are monitoring and maintaining the network. With the two groups of users and admins working together, work can be completed while maintaining the companies high network standards.

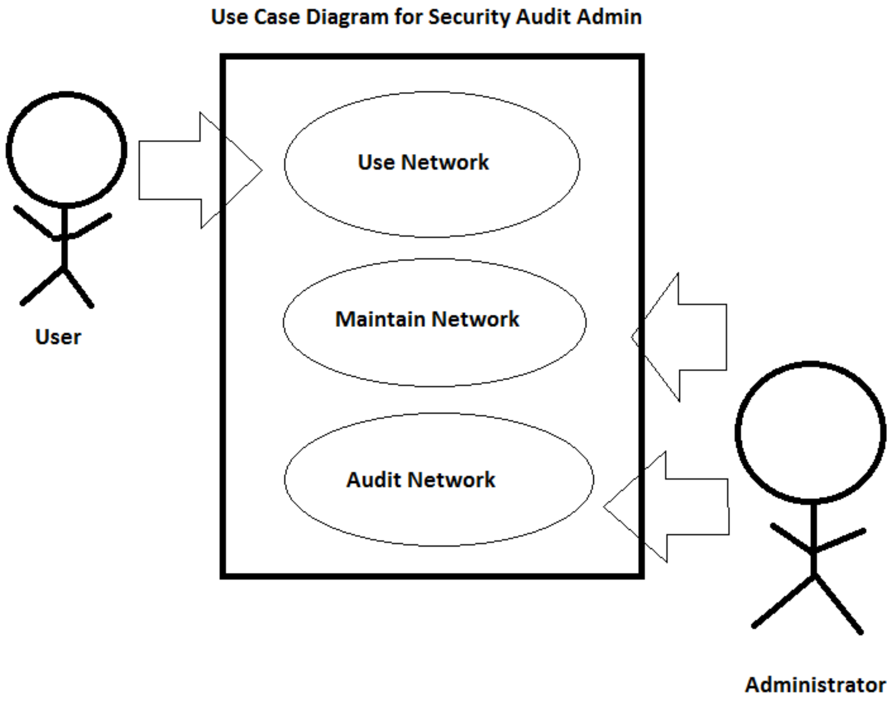


Figure 9.

User Profile

The user profile below shows the potential users of this project and the skills that they might have. Figure 10 below helps show what experience level that the users using this project might have and what background they should have.

User Profile
Application: Conducting an IT security audit
Potential Users Network Admins, CIO, Director of IT, anyone tasked with performing a security audit.
Software and Interface Experience: User will need to know about everything on the network they are working on.
Experience with Similar Applications: The user conducting the audit must have prior audit experience.
Task Experience: Users will be able to go through known security issues and with a team implement solutions.
Frequency of Use: Once a quarter
Key Interface Design Requirements that the Profile Suggests: The user will need a background in network security. The user will need to meet with heads of each team such as database, networking, software, developers. Users will need to put into place a solution to resolve the issues being examines by the IT security audit.

Figure 10

Future Recommendations

This senior design project addressed two major areas that needed improvement in the company. While these solutions are a great start, there are additional areas that should be addressed in the future. An employee security training program could be put into place to help educate employees about common security threats they may see on a daily basis while doing their job. With a training program put into place employees will also know what to do in each of the situations they might face. The actions employees take when faced with these situations will help in keeping security levels up while decreasing work for the in house IT department. To go along with the employee security program, a program about physical security would assist in eliminating unauthorized people gaining access to the building. A focus on this area would help the company maintain outstanding security levels both from a network and physical point.

Conclusion

During the implementation of the project there were many challenges, both good and bad. The project allowed development of professional skills including project management. My communication and planning skills were put to the test for this project. One of the most difficult tasks was actually getting meetings to happen on time and when they needed to happen. Although the budget of this project may have been a little steep, the money invested could possibly save the company millions of dollars in the future. If these problems were not addressed as we speak a disgruntled employee could be going through their account information, saving all of their old emails, and taking all of their customer's information. After some time goes by they could start their own business and potentially take millions of dollars in business away from TQL. Being proactive about these situations will save the company time, resources, and most of all money. If resources do not have to be used to solve the problems that could potentially happen, they can be applied towards other tasks such as making more money. This project helps further protect TQL both from a network side and physically. The millions of potential dollars saved due to this project could fund the opening of many future satellite offices and allows the company to expand its national footprint even further. The skills that were learned during this project will help me in future projects and work experiences down the road.

References

"Security Audit - IT Security." *Security Audit - IT Security*. Ziff Davis, 2013. Web. 07 Oct. 2013.

"Security Auditing." *Windows Server Security Auditing*. Microsoft, 25 Jan. 2010. Web. 7 Oct. 2013. <http://technet.microsoft.com/en-us/library/cc771395%28v=ws.10%29.aspx>.

Page, Pam. "Security Auditing A Continuous Process." *Sans.org*. SANS, n.d. Web. 7 Oct. 2013. <http://www.sans.org/reading-room/whitepapers/auditing/security-auditing-continuous-process-1150?show=security-auditing-continuous-process-1150&cat=auditing>.

Hayes, Bill. "Conducting a Security Audit: An Introductory Overview." *Endpoint, Cloud, Mobile & Virtual Security Solutions*. Symantic, n.d. Web. 07 Oct. 2013. <http://www.symantec.com/connect/articles/conducting-security-audit-introductory-overview>.

Lakshmana Rao Vemuri. "Preparing for the Security Audit - Recommendations for Beginner IT Auditors." *Preparing for the Security Audit - Recommendations for Beginner IT Auditors*. Internal Auditor, 4 Nov. 2013. Web. 07 Oct. 2013. <http://www.theiia.org/intAuditor/itaudit/archives/2006/april/preparing-for-the-security-audit-recommendations-for-beginner-it-auditors/>.

Val Thiagarajan. "Information Security Management." *Www.sans.org/score/checklists/ISO_17799_2005.doc*. SANS, n.d. Web. 7 Oct. 2013.

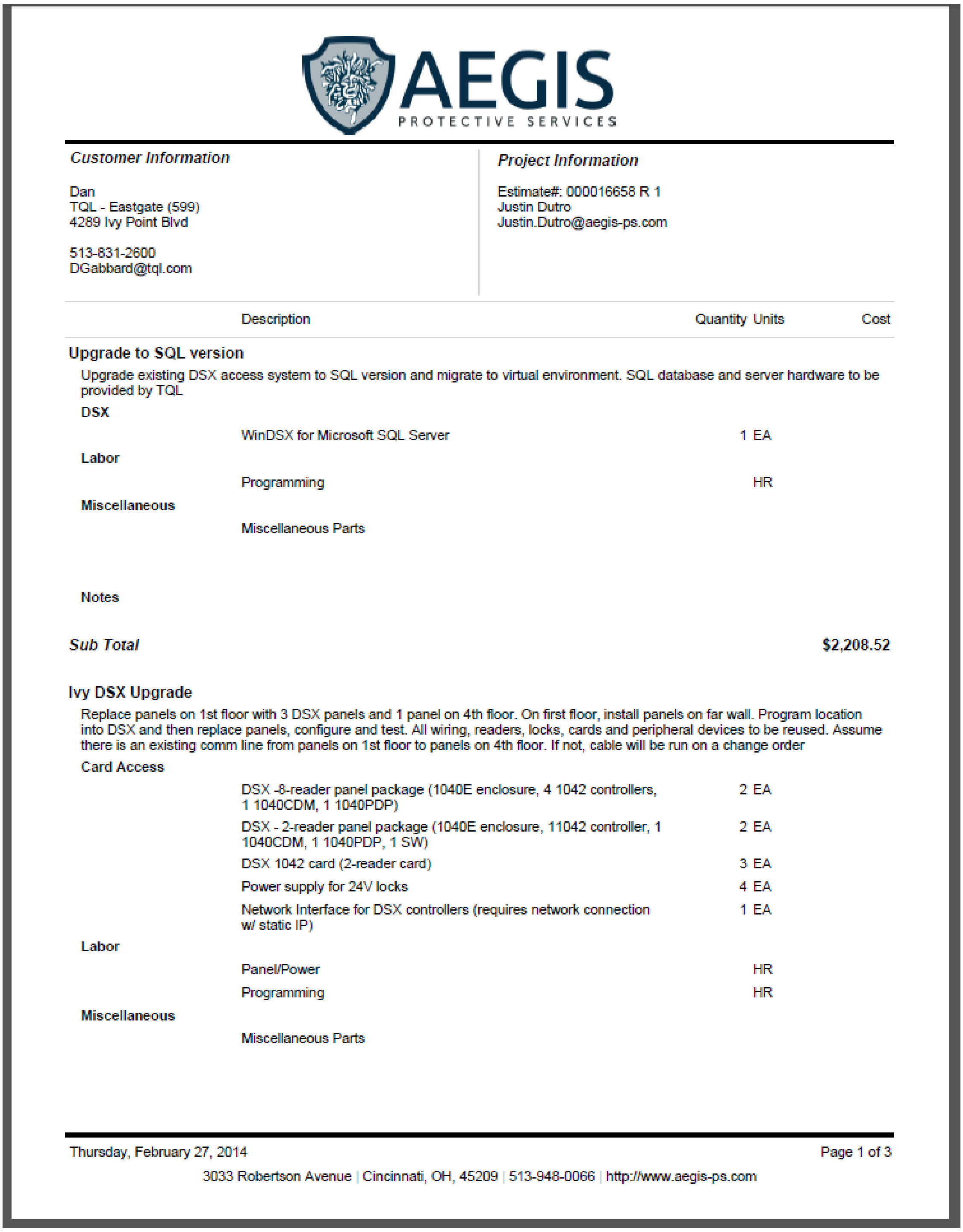
Carole Fennelly. "IT Security Auditing: Best Practices for Conducting Audits." Editorial. *IT Security Auditing: Best Practices for Conducting Audits*. Tech Target, n.d. Web. 07 Oct. 2013. <http://searchsecurity.techtarget.com/IT-security-auditing-Best-practices-for-conducting-audits>.

Cobb, Michael. "Best Practices for Audit, Log Review for IT Security Investigations." *Best Practices for Audit, Log Review for IT Security Investigations*. Computer Weekly, n.d. Web. 07 Oct. 2013. <http://www.computerweekly.com/tip/Best-practices-for-audit-log-review-for-IT-security-investigations>.

Raposo, Marco. "Security Audit Best-Practices." *Security Audit Best-Practices*. Slideshare.net, n.d. Web. 07 Oct. 2013. <http://www.slideshare.net/mhraposo/Linked-in-Audit-Presentation>.

Semple, Blair. "Preparing for a Security Audit: Best Practices for Storage Professionals." *Http://www.snia.org/sites/default/education/tutorials/2009/spring/security/BlairSemple-Preparing-for_Storage_Security_Audit.pdf*. SNIA, n.d. Web. 7 Oct. 2013.

Appendix A



AEGIS
PROTECTIVE SERVICES

Customer Information

Dan
TQL - Eastgate (599)
4289 Ivy Point Blvd

513-831-2600
DGabbard@tql.com

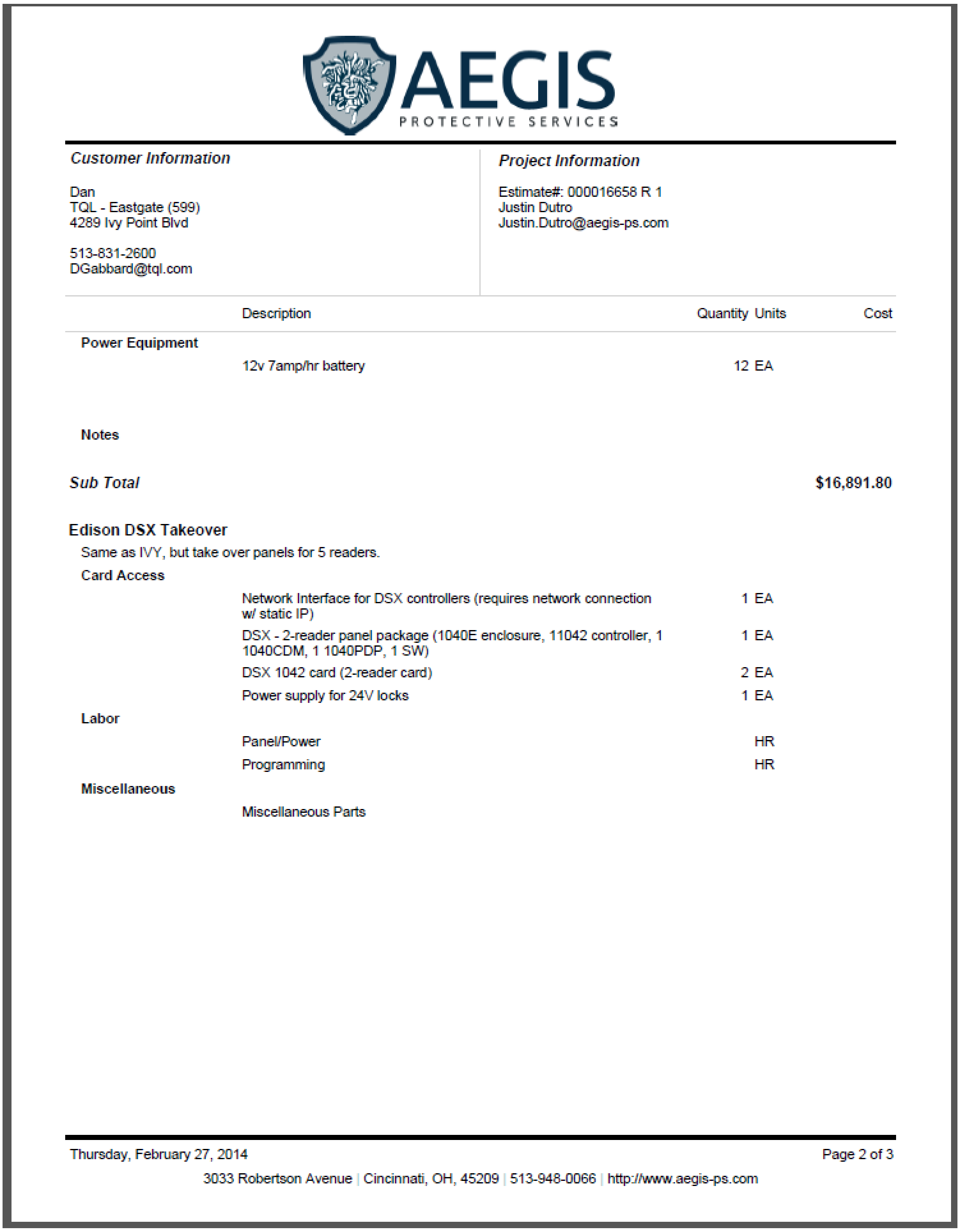
Project Information

Estimate#: 000016658 R 1
Justin Dutro
Justin.Dutro@aegis-ps.com

	Description	Quantity	Units	Cost
Upgrade to SQL version				
Upgrade existing DSX access system to SQL version and migrate to virtual environment. SQL database and server hardware to be provided by TQL				
DSX				
	WinDSX for Microsoft SQL Server	1	EA	
Labor				
	Programming		HR	
Miscellaneous				
	Miscellaneous Parts			
Notes				
Sub Total				**$2,208.52**
Ivy DSX Upgrade				
Replace panels on 1st floor with 3 DSX panels and 1 panel on 4th floor. On first floor, install panels on far wall. Program location into DSX and then replace panels, configure and test. All wiring, readers, locks, cards and peripheral devices to be reused. Assume there is an existing comm line from panels on 1st floor to panels on 4th floor. If not, cable will be run on a change order				
Card Access				
	DSX -8-reader panel package (1040E enclosure, 4 1042 controllers, 1 1040CDM, 1 1040PDP)	2	EA	
	DSX - 2-reader panel package (1040E enclosure, 11042 controller, 1 1040CDM, 1 1040PDP, 1 SW)	2	EA	
	DSX 1042 card (2-reader card)	3	EA	
	Power supply for 24V locks	4	EA	
	Network Interface for DSX controllers (requires network connection w/ static IP)	1	EA	
Labor				
	Panel/Power		HR	
	Programming		HR	
Miscellaneous				
	Miscellaneous Parts			

Thursday, February 27, 2014 Page 1 of 3

3033 Robertson Avenue | Cincinnati, OH, 45209 | 513-948-0066 | http://www.aegis-ps.com



AEGIS
PROTECTIVE SERVICES

Customer Information

Dan
TQL - Eastgate (599)
4289 Ivy Point Blvd

513-831-2600
DGabbard@tql.com

Project Information

Estimate#: 000016658 R 1
Justin Dutro
Justin.Dutro@aegis-ps.com

	Description	Quantity	Units	Cost
Power Equipment				
	12v 7amp/hr battery	12	EA	
Notes				
Sub Total				**$16,891.80**

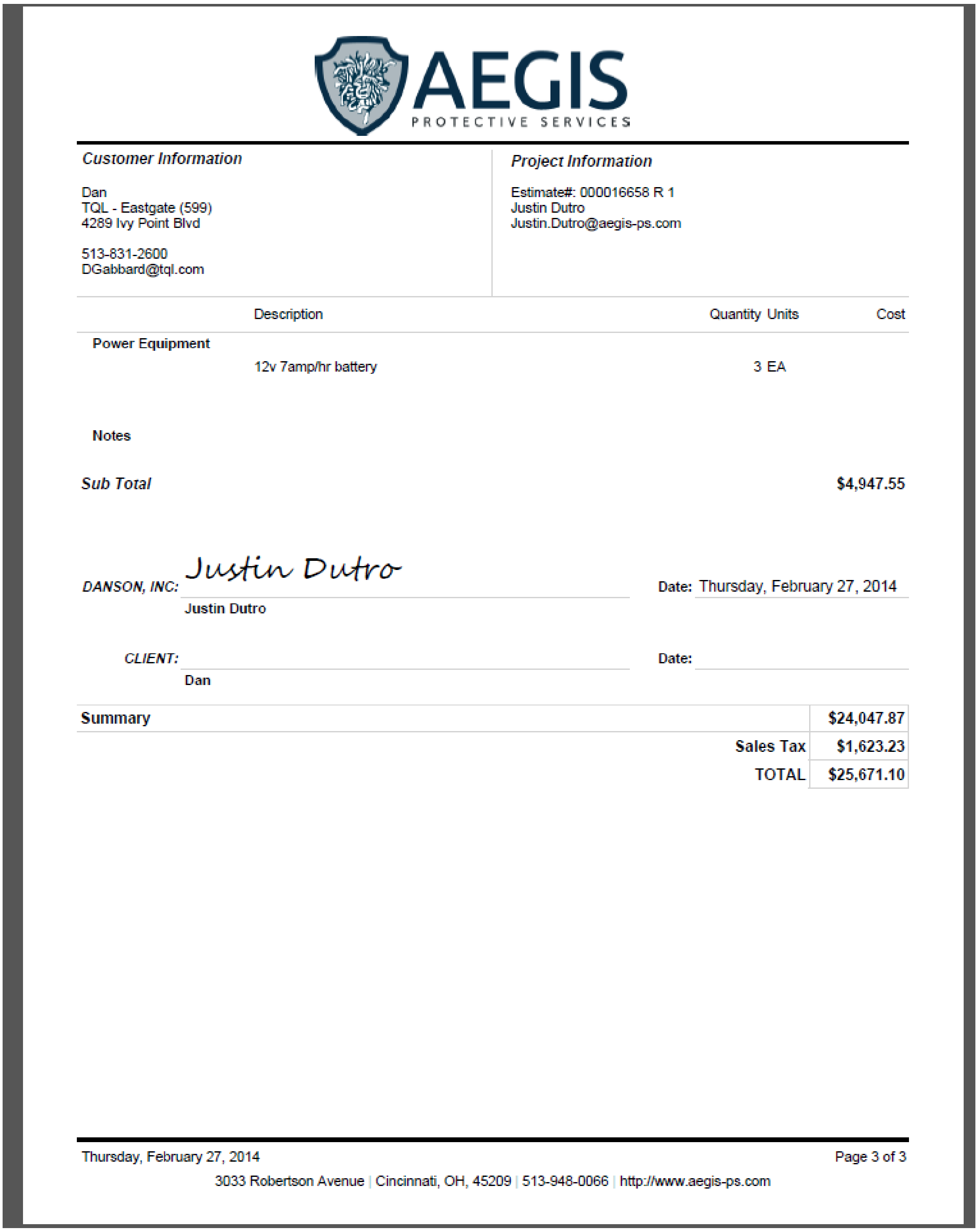
Edison DSX Takeover

Same as IVY, but take over panels for 5 readers.

	Description	Quantity	Units	Cost
Card Access				
	Network Interface for DSX controllers (requires network connection w/ static IP)	1	EA	
	DSX - 2-reader panel package (1040E enclosure, 11042 controller, 1 1040CDM, 1 1040PDP, 1 SW)	1	EA	
	DSX 1042 card (2-reader card)	2	EA	
	Power supply for 24V locks	1	EA	
Labor				
	Panel/Power		HR	
	Programming		HR	
Miscellaneous				
	Miscellaneous Parts			

Thursday, February 27, 2014 Page 2 of 3

3033 Robertson Avenue | Cincinnati, OH, 45209 | 513-948-0066 | http://www.aegis-ps.com



AEGIS
PROTECTIVE SERVICES

Customer Information

Dan
TQL - Eastgate (599)
4289 Ivy Point Blvd

513-831-2600
DGabbard@tql.com

Project Information

Estimate#: 000016658 R 1
Justin Dutro
Justin.Dutro@aegis-ps.com

	Description	Quantity	Units	Cost
Power Equipment				
	12v 7amp/hr battery	3	EA	

Notes

Sub Total	**$4,947.55**

DANSON, INC: Justin Dutro
Justin Dutro

Date: Thursday, February 27, 2014

CLIENT:
Dan

Date:

Summary		**$24,047.87**
	Sales Tax	**$1,623.23**
	TOTAL	**$25,671.10**

Thursday, February 27, 2014 Page 3 of 3
3033 Robertson Avenue | Cincinnati, OH, 45209 | 513-948-0066 | http://www.aegis-ps.com