University of Texas at San Antonio

Roadrunner Custom Tees

Securing Network Access

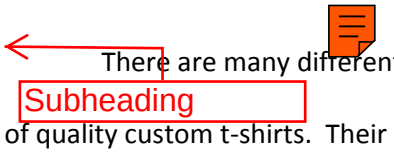
Chris Bailey, Paul Reimann, Matt Gonzales, Cannon Benson, and Brandon Taylor

Fall 09

Table of Contents

Roadrunner Custom Tees is a web-based vendor that sells custom t-shirts. Roadrunner Custom Tees hosts their website and maintains all the equipment associated with the website. They only use services from credit card companies and mail companies in conjunction with their website. Roadrunner Custom Tees uses designs that are submitted online by customers and employees for their t-shirts and then are screened to comply with copyright and other related laws. After a design is approved it is then stored in the company database to be use in the t-shirt creation process. If a design is a customer's own creation they have an option to not allow their design to be viewable to the public. These designs can be then viewed by other customers later to be selected for purchase. Once the customer chooses the designs they desire they can then check out and pay for their t-shirts using a credit-card and choose their method of shipping.

Roadrunner Custom Tees has been in business for 5 years and is stationed in San Antonio, Texas. Roadrunner Custom Tees believes customer service is very important and maintains polices and standards to maintain good customer relations. There are about 75 people that work for Roadrunner Custom Tees and are considered to be valued members. This company has grown quickly in the past 5 years slowly adding new members and equipment to deal with the demand. Quality materials have high importance in the creation of the company's t-shirts and are used to create long lasting products.



There are many different stakeholders in this company that all have a vital roles in the creation of quality custom t-shirts. Their of course is the owner whose vision and leadership allowed the company to first form and continue to grow into the business it is today. The managers oversee different aspects of the t-shirt creation process like the sales portion, production, financial, and the customer service side of the company. These managers make sure their part of the company run efficiently and cost effectively. The employees of the sales function of the company deal with advertising, marketing, and making decisions to help the company grow. The financial employees

oversee the online transactions, deal with credit card companies, and perform other financial/accounting duties. The production side of the company focuses on taking orders and creating the t-shirts to customer specification. The production side also has a few designers that create t-shirt designs for the company to use to sell t-shirts. The customer service employees answer calls and answer customer's questions and complaints to ensure that the customer is satisfied with their purchase. These stakeholders have an impact on security relative to the areas that they work in. For example the financial employees who have control of much of the company's finances have a direct impact in that area.

In addition to these groups are the technicians and administrators that maintain and secure the information technology of the company. This group includes the network administrator and security professional that play a managerial type role in overseeing the computer technology in the company. In this group there are the webmaster, database administrator, help desk, and general technicians who maintain the different technologies that make this web-based company function. This group of stake holders have a high impact on security in that much of what they do gives them elevated privileges in the company's computer systems and therefore have more opportunities and power to directly affect the security of the company's systems.

There also other important stakeholders that make the company what it is today some of which include custodial staff, general assistants, and others that don't have a direct role in t-shirt creation. Another important group of stake holders is of course the customers who also help by supporting the company with their business and t-shirt designs. These stake holders should have limited impact on the security of the company due to their limited access to the company's systems. All these stake holders are important to the company in order to continue the growth of Roadrunner Custom Tees.

Subheading

Several network interfaces that might impact security will need to be considered. Input fields on the website could be used to circumvent security and exploit data. Such data could be stored customer information, unannounced products, or other non-public information. Physical interfaces between networked servers could also pose a possible security risk if not monitored. Eavesdropping is a possible concern if appropriate encryption schemes are not used when potentially sensitive data is being transmitted between interfaces.

Subheading

In addition, regulations and legislation will need to be addressed. As a standard rule, a Data Use Notice will be available for viewing. Also called a Privacy Policy, this notice will explain and describe how and of which data we plan on retaining, processing, disclosing, and purging as well as the security measures taken to protect such personal information.

Compliance with the Children's Online Privacy Protection Act will also need to be met. Brought into effect in April of 2000, the COPPA deals with the online collection of personal information by entities or persons under United States jurisdiction from children under the age of 13. It explains what we as an online operator must include in our privacy policy, how and when to seek verifiable parent or guardian consent, and what responsibilities we as an operator have to protect children's privacy and safety online as well as what restrictions on marketing there are to those under this age. Violations for not complying with this act can result in hefty fines. In order to prevent such fines, Roadrunner Custom Tees will require children to get verified parental consent before we gather and use any personal information received.

Another law that will be put into consideration is the CAN-SPAM Act. Making its appearance in December of 2003, the CAN-SPAM Act established the United States' first national standards for the sending of commercial e-mail requiring the Federal Trade Commission to enforce its provisions. The act defines a commercial electronic mail message as any electronic mail message the primary purpose of

which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose). The term "Commercial", by many industry standards, is most often defined by a combination of both the content in the subject line and "above the fold content" in the body of the message. If this content contains a solicitation and it can be determined that the majority of the content is selling something, it is a commercial offer. The bill permits e-mail marketers to send unsolicited commercial e-mail as long as it adheres to 3 basic types of compliance defined in the CAN-SPAM Act: unsubscribe content and sending behavior compliance.

Compliance with the unsubscribe portion requires a visible and operable unsubscribe mechanism to be present in all emails. Consumer op-out requests must be honored within 10 days of being received. In addition opt-out lists, also known as suppression lists, must only be used for compliance purposes.

Content compliance requires that accurate from lines be used at all times. Relevant subject lines must also be used in accordance to body content and must not be deceptive in any way. Included in the message must be a legitimate physical address of the publisher and/or advertiser.

Sending compliance requires that a message not be sent through an open relay, be sent to a harvested email address, or contain a false header. Falsifying a header is considered a serious violation and generally indicates criminal or malicious intent, which can bring the attention of other law enforcement agencies.

Our company will comply in full by using accurate header information as well as use a subject line that accurately reflects the content of our messages. We will identify all advertisement messages as an ad and tell recipients how to opt out of receiving future email relating to such content. Opt-out requests will be handled promptly and we will monitor what others are doing on our behalf to ensure that proper handling is being done.

One of the tradeoffs of running a business that operates almost exclusively through the Internet and web applications is a need for enhanced security for the supporting technology that is used. Since the business operates solely via the Internet, using a storage warehouse to manage inventory, it is imperative that Roadrunner Custom Tees secures both of these sections of the business process to ensure safe and reliable services to the customer. Roadrunner Custom Tees will need to consider the threats and vulnerabilities that are inherent in this particular business setting such as SQL injections on the web application front, information security with regard to customer information, inventory protection and other topics that are relevant to an Internet business.

To begin, it is important that Roadrunner Custom Tees first delves into the security of the online applications and transaction system. SQL injections are a major security threat to Roadrunner Custom Tees' system because as an online retailer, they are forced to provide means for customers to purchase their products since they do not have a typical brick-and-mortar setup that offers a physical location for order processing. These kinds of attacks are relevant to Roadrunner Custom Tees because web applications run with a database in the back that stores and processes the SQL commands which allows the business to maintain records, store user information, order information and other necessary data. A SQL injection attack is a malicious act carried out by a user who has the knowledge to submit certain syntax into user input fields such as name, e-mail and phone number to manipulate the SQL statement being run in the background to gain information from the database. These statements, when manipulated, can be written to provide all of the information within a database or just certain data fields depending on the security of the input and overall application code.

In addition to SQL injections, another form of attack is the man in the middle threat. Since Roadrunner Custom Tees will be using the internet and relevant applications to handle business transactions, Roadrunner Custom Tees must also consider such threats as cross-site scripting and

session hijacking. Cross-site scripting is a method by which a malicious user can use data input fields, much like SQL injection attacks, to insert harmful code into a web application. These segments of code are then executed and can do anything from redirecting a user's browser to a fake, imitation website in an attempt to confuse the user and convince them to enter their personal information or obtain private information stored in cookie files. This could potentially allow an attacker to obtain customer information or fraudulently obtain customer money. Similarly, session hijacking allows for a man in the middle to take control of a user's session while it is in progress. Session hijacking is the act, by a malicious user, of brute-forcing, re-engineering or simply capturing a session ID that is used to identify a customer's successful login. With this information, an attacker could use their credentials to make purchases to obtain information about the customer that may otherwise be unavailable. Both of these threats are major security threats to Roadrunner Custom Tees because it not only exposes customer data to outsiders, but these attacks could also weaken the security reputation of the business which may result in a decline in sales and trust.

Moving away from the web environment to physical security, Roadrunner Custom Tees owns a storage warehouse where orders are sent and processed. This warehouse contains the entire inventory for the business so it is vital that it is protected both from a cost perspective as well as customer satisfaction. When an order is sent to the warehouse to be processed, employees must participate to some degree to complete the order. Additionally, we must ensure that the inventory is not tampered with, stolen or otherwise degraded with respect to quality. With that said, Roadrunner Custom Tees must do a security analysis to determine the most efficient approach to securing this warehouse from physical threats.

Last, another important physical threat to our company is the employees themselves. Although a large portion of the business takes place online, there is still a necessity to employ people to operate

the computers, maintain the equipment and website as well as handling the order processing and shipment of orders. Roadrunner Custom Tees must ensure that disgruntled or careless employees to not misuse tamper with or otherwise expose customer or business information. It is important that Roadrunner Custom Tees does not allow these kinds of physical threats to go unnoticed. If employees are able to cause harm to the system at any particular level or process, the impact could be far-reaching and disastrous for the business. Customer or business information could be compromised, orders may be lost and overall customer satisfaction will decline.

Although some major threats have been covered, there are various other threats and vulnerabilities that may still affect Roadrunner Custom Tees even if the impact is indirect. For example, the company that provides web hosting may have a server or power outage, software updates may be overlooked on the hosting company's end, natural disaster's may harm the warehouse or connection somewhere between the customer and our website or something as random as a car crashing into a power line that carries a piece of our connection. In this particular case, it is necessary that Roadrunner Custom Tees focuses on the threats and vulnerabilities that have been discussed. Concentrating on these specific threats will provide a relatively safer and more secure means of operating in this business setting.

In today's society, it's difficult knowing who / what you can trust. If we could trust everyone and everything there would be no need for security. We could simply leave our doors unlocked and live without fear. Unfortunately, this isn't how things normally operate. There will always be someone or something attempting to cheat the system. Now the question is; how does one prepare for these types of situations? For example, would you rather leave a door unlocked, let something get stolen, and then deal with the consequences? Or would you rather take the time to create a plan on how to protect your assets? Roadrunner Custom Tees, as many should, chose to be proactive rather than reactive.

As previously stated, Roadrunner Custom Tees deals with many online transactions during everyday business which are transported over the Internet. It is essential that they properly secure this information. To help prevent these attacks, Roadrunner Custom Tees has taken the following measures. First, they prevent unauthorized access to the database and limit the permissions that are granted to the account that the application uses. Second, Roadrunner Custom Tees validates user input properly before using it, thereby stripping off the potentially malicious portions. Thirdly, they always use parameterized SQL queries and stored procedures rather than building SQL statements dynamically. (Aspnetpro) With any company, vital information should be on a need to know basis. For this reason, Roadrunner Custom Tees avoids displaying the actual database errors and/or messages to the end users. This helps prevent vulnerabilities and potential attacks.

Previously mentioned, man-in-the-middle attacks are a possibility that concerns almost every online entity. To prevent session hijacking Roadrunner Custom Tees uses long random numbers as their session keys which will drastically cut down on success rates via brute force attacks. Customers have a tendency to be impatient so Roadrunner Custom Tees tries not to continually send checks of identity to the user. One of the most successful techniques in their security is through using encryption via SSL. This eliminates hackers being able to sniff out customer information. This company also uses Network Intrusion Detection, firewalls, and antivirus. It is imperative that all patches are up to date and properly tested for business survival.

Roadrunner Custom Tees not only focuses on logical controls, but also physical controls to protect their assets. Both work as one to safeguard their company assets. To know what to protect, one must first consider the value of their assets. As a t-shirt manufacturer, Roadrunner Custom Tees has many assets that are critical to business continuity. Their accounting / administrative offices contain computers used for E-commerce. Vital information is passed through and stored on these computers on

a daily basis. They also have a design studio where artists digitally create new designs for their product. If those computers were compromised, they'd be selling blank t-shirts. Their assembly line, printing machines, data center and logistics departments also play a role in security planning.

Physical security controls are simply a way of protecting Roadrunner Custom Tees' buildings, employees and tangible assets. Because they operate from a warehouse, they have less risk of customer theft. This however, doesn't entirely rule out the possibility of theft. Employees often get comfortable with the way things are run and feel that they can get away with anything. To prevent possible theft, Roadrunner Custom Tees have installed security cameras throughout the building. The cameras are placed in: high-traffic areas, entry / exit doors, data center, and administrative / logistics offices. The feed is recorded to DVD and the files are kept for one month before being re-written. If a problem is discovered, proper authorities will be notified. While constantly dealing with electronic devices, there will always be a chance of fire. If such an event happens, Roadrunner Custom Tees has a fire detection system in place to prevent catastrophic loss.

Upon entry of Roadrunner Custom Tees' warehouse, you will find a lobby, help desk and two additional doors. Each door has a card-entry system. If there is a problem with a card, the help desk can confirm identity provide an override. The left door leads to their logistics office and production area. The right leads to their: data center, design studio, and administrative office. Both sides are equipped with restrooms, break rooms, and storage / custodial closets. Employees are often overlooked as being the most important asset to a company. To protect employees, there are fire exits in proper locations. All exterior doors are constructed with re-enforced steel and will sound an alarm if vigorously opened. The main entrance provides a keypad for their intrusion detection system. Only management has the code to this alarm and only they hold the key to the door. This provides a form of two-factor authentication. To prevent vehicles from driving through their entryway, there are several polls outside

the entrance. Because Roadrunner Custom Tees does not operate 24 hours a day, they provide proper lighting where needed. Through the building you will find storage closets for general and custodial supplies. This will prevent unnecessary placement of items in high-traffic areas.

Each office containing valuable assets such as desktops, pen tablets and monitors will be secured with the same card-entry system. Employee ID cards will allow access to necessary offices and will be kept in a log for future audits. This isn't always a full proof method of security, because one could simply hold the door open for a partner in crime. To help with this issue, computers are tethered to their desks to prevent theft and/or relocation. Also, employees aren't allowed to bring food and drink into the offices due to the chance of accidentally damaging assets. To offset this, while keeping employees happy, Roadrunner Custom Tees provides fully furnished break rooms. Keeping employees happy is a good way to prevent disgruntled attacks. Awareness training is provided to keep employees informed on their responsibilities.

Computer and network security concerns are growing at rapid rate compared to the past. As the reliance on computing and networking steadily increase, to include practically every business transaction conceivable, the importance of protecting our computer and network infrastructure for processing business transactions is more vital than ever. Information security, in the Internet's early structure, was a rare subject given very little consideration recent attacks have opened our eyes. Recent security incidents involving billions of dollars and numerous resources lost has consequently forced us to create a whole new field in the Information Technology profession. This new and exciting opportunity has become known as Information Assurance.

Designing a proper and effective incident handling response plan should be a proactive rather than reactive decision and was given a great deal of thought at Roadrunner Custom Tees. While most companies will be lucky not to have to use this plan, studies show that companies who have a clear

incident response plan have their damages minimized when an attack does occur. Designing an accurate and effective incident response plan is not an ordeal that takes place overnight, a great deal of thought and planning needs to go into the incident response plan and will be a unique result for every organization based upon their policies and business practices. Nevertheless, discussions between executive and technical personnel need to take place to determine the responsible party, the notification party or team, and best practices to mitigate the damage and learn from the experience.

Ideally, the CIO, CTO, or other top-level technology professional should devote an adequate amount of time and resources to construct an incident response team, comprised of members with a variety of different skill sets to handle different situations as they arise. This team needs to be diverse and well trained in order to deal with questions that will be asked by various entities, internally and externally. As a good rule of thumb, any personnel who are not normally authorized to speak to the public regarding company confidential information should also be excluded regarding response to incident situations.

Once the incident handling response team has been established, a thorough analysis and evaluation should commence to determine Roadrunner Custom Tees current intrusion detection system. If one has never been implemented, this would be an ideal time to evaluate all the potential security threats and make a well-informed decision to acquire a network intrusion system (NIDS). The NIDS chosen will need to be very versatile, run continuously without interaction, free from performance bottlenecks, able to adapt to a dynamic environment, and the ability to recover from a failure or fault tolerant. While the perfect NIDS probably does exist, Roadrunner Custom Tees determined their critical needs and purchased the NIDS based on those needs and requirements.

After the NIDS was implemented, a workflow of action events was created. This event action plan assessed the possible repercussions from an incident and action precedence procedure was taken

based on corporate policy. In the event a security incident does take place, the proper personnel (incident handling response team) should be notified immediately and the proper action steps should be followed to assess the damage and further contain the incident. Once the damage has been carefully assessed, an action or decision should be made on how to proceed. Based on this procedural decision, the proper action should be taken to eradicate the threat while preserving the optimal amount of information and details in the event that law enforcement interaction is deemed necessary.

Some of the primary goals of incident handling and response techniques is to preserve critical data, minimize down time, and becoming more adept from the experience to improve on future responses. In a perfect world, the need to respond to security incidents will never have to take place but, threats are a major problem for all levels of organizations and the proper security measurements and equipment should be implemented in order to mitigate the damages. There's an old saying that says, "If a hacker really wants to get into your system, he will". Unfortunately, this statement is very accurate and undeniable. Sadly, your best line of defense is often to configure your network infrastructure a sufficient amount in hopes the attacker will move on to an easier target.

Networks are the essential element in terms of business communication and production in a technology, setting for today's globally competitive world. At their inception, networks were simplistic in design and extremely insecure due to their intention. The initial networks were created to simply share data and resources and were used in a small scale environment, often referred to as peer-to-peer or workgroup networks. These small networks worked well for a small amount of users but, were not ideal for a large amount of users. To offer a more scalable solution, client-server networks were formed and offered a central resource destination or server where the clients could access shared resources and benefit from interconnectivity. These two advents would prove to be a solid foundation for an innovative technology that would change the world as we knew it, the birth of the Internet.

Without a doubt, the Internet has completely transformed our lifestyle and has made business and communication easier. With this convenience, it unfortunately created a onslaught of security threats and holes that could possibly be used as a malicious assault. The Internet is the largest globally interconnected network, and anyone who uses it should be properly protected. This is unquestionably the case for Roadrunner Custom Tees, where the entire business model and practice is reliant upon this technology.

The corporate network at Roadrunner Custom Tees communicates to the outside world by utilizing a bonded T1 connection provided by a local telecommunications presence in the San Antonio area. The connection is made available by combing three individual T1 circuits and configuring them to be bonded or act as a single connection. This bonded configuration is made possible using a Cisco 1800 router and not only provides increased bandwidth but also provides a simple fault tolerant solution. Roadrunner Custom Tees can continue its business in the event of a single or even a double T1 failure, although bandwidth performance will suffer significantly. Placed directly behind the router is a Cisco PIX firewall that is configured using the least privilege mentality, only required ports and protocols necessary for business communication is allowed. The firewall is configured in a three tier fashion using a demilitarized zone (DMZ) to separate its Internet facing servers from its internal network. To counter attack against well-known threats and attacks, broadcasting traffic has been disabled and filters enabled on the corporate firewall. In addition, the firewall log is monitored immensely by the network administrator and his subordinates.

The internal corporate network at Roadrunner Custom Tees is handled by Cisco Catalyst switches as well as fiber optic and category 6 cabling throughout its facility. The datacenter is physically secured by cameras, badge access, and locked doors that only critical personnel have keys to. The internal network equipment is managed and maintained by our network staff at Roadrunner Custom

Tees, is password protected, and accessed only in a secure manner using the secure shell protocol. All switches are monitored regularly and port security is enabled allowing only specified media access control addresses connectivity.

Works Cited

http://aspnetpro.com/newsletterarticle/2006/12/asp200612jk_l/asp200612jk_l.asp

http://projects.webappsec.org/SQL-Injection

http://projects.webappsec.org/CrossSiteScripting\

http://www.imperva.com/resources/glossary/session_hijacking.html