PDSA.com

*Solutions for the Real World*

# PDSA Special Report

# Is your Company's Security at Risk

# Special Report Is your Company's Security at Risk

## Introduction

There is probably no such thing as a completely secure company. However, if you are not thinking about security in your company, you are running a big risk. We are not just talking about application security or web site security. What are these other risks? How about stolen data, stolen equipment, lost business, or even worse, lawsuits due to not securing private customer data? You need to start doing some planning and coming up with a security threat assessment for your business. This will include all areas such as physical security, network security, web site security and data security.

## The Truth about Security

Security is hard to do. Whether it is security to lock down applications/servers, or physical security, we are only as good as the tools and the people using those tools. There are many tools to help us, but they are all disjointed, separate products. There are many security companies that can help us lock down our facilities, but if everyone does not participate, then you are only as secure as your weakest link. While it is impossible to be 100% secure, you have to know and understand all the known threats and be resilient to new attacks as well as you can.

Another important aspect of security is that it is symbiotic. This means that all the pieces have to work together in order to be the most secure. This means from your point of entry to your building all the way through you network, web servers, file servers, and even your physical machines you must have a comprehensive security plan for dealing with possible intrusions. Security must be designed from the beginning; otherwise you are just patching something that is already broken. This can lead to many weak links in your process.

## Types of Threats

There are many types of security threats you need to consider when creating your threat assessment plan. The most obvious one many people think about these days are outside threats like viruses and hackers. But there are just as many, if not more, threats coming from the inside. What about someone stealing a computer, turning off a critical server, stealing passwords or sensitive data to sell to a competitor, changing data, or stealing credit card data from your ecommerce site? All of these are threats that need to be

considered and mitigated in your security plan. Remember, threats can come from outsiders like hackers, but also insiders like employees, contractors and even delivery persons.

## Goals of a Security System

It is important that you set some up front goals for your security system you will put in place. These goals should include the following:

1. Ensure people can only get to where they need to in order to perform their jobs.
2. Ensure malicious code does not run on computers by employing virus scanners.
3. Ensure physical machines are protected.
4. Protect all entry points into your environment. This includes access to building, server rooms, and into your network.
5. Identify all potential threats and try to nullify them. These include internal, external, technical and physical threats.

## Physical Security Considerations

There are a few different physical security aspects you should always be looking at when designing your security plan. Below is a list of considerations to look at when designing your physical security system.

1. Access to your building. How secure is the building you are in. Do you need a security guard at the front, or can your receptionist work as your gatekeeper.
2. User identity theft. Would it be possible for User A to use User B's machine to perform a theft of data, but then the User A is blamed for it? If so, then you need to enforce auto time-out of your windows sessions to help reduce this threat.
3. Passwords need to be secure. Sometimes a physical audit of people's workstations is needed to ensure that no one can discover another person's identity. Ensure people are not writing down passwords on pieces of paper, or storing passwords within a file on their hard disk.
4. Access to different rooms within your building. Do you have some departments that do more sensitive work? If so, then that department's physical offices should have a separate lock from the rest of the building.

5. Access to servers that run your business. This includes your network servers, database servers, web servers or any other critical machines. Most critical with this is to ensure that a limited amount of people have access to these machines. They should be locked behind a separate door. In addition, the physical machines themselves, or the racks upon which they reside need to be locked down as well. It would be best to make sure that the people that have access to the room do not have access to remove the machines from that room. Terminal services to the machines in that room should be very limited. Ensure there is no wireless access to the machines within this room. Be sure that any USB ports are turned off. This eliminates the threat of people using USB keys to remove data. In addition, make sure the On/Off switches on the machines cannot be accessed by anyone without access to cage in which the machines are located.

## Publish your Security Procedures

It is very important to communicate exactly what your security policies are to your employees, and even your customers. By raising the awareness of security among your employees and customers, people will feel more secure within your company, and your customers will gain a healthy amount of respect and feel secure about giving you their private information when doing business with you. For your employees it is very important that you inform them what you expect from them to help the company enforce these security policies. Remember, you are only as secure as your weakest link. Be sure to publish the consequences of not following security procedures correctly. If there are consequences spelled out in writing, then you can avoid wrongful termination lawsuits, or privacy violations that will foster decreased customer loyalty. These types of things can cost a business a lot of money and must be taken very seriously.

## Summary

Security should be an important priority for all businesses. If not, you might find yourself on the wrong end of a lawsuit, or out of a job because of loss of valuable business to a competitor. Create and enforce a security policy at your place of business. It might even be advisable to hire a third party company to help you create security policies for your company.

PDSA has a complete Security Audit where we perform an exhaustive checklist against your applications and identify areas where you could potentially have security issues in your applications and your databases. We then provide you with a written report and give you some remedial action you can take.

# Contact Information

If you would like to know more about the information in this special report, please contact either Paul D. Sheriff or Michael Krasowski at PDSA.

Paul Sheriff

(615) 675-4632

PSheriff@pdsa.com

Michael Krasowski

(714) 734-9792 x223

Michaelk@pdsa.com

## Company Information

PDSA, Inc.
17852 17th Street
Suite 205
Tustin, CA 92780

**Tel** (714) 734-9792
**Fax** (714) 734-9793
www.pdsa.com

PDSA.com
*Solutions for the Real World*