



# The Internet Security Risks Facing your Organization: Test and be Saved

Last Updated: 15th January, 2009



## Introduction

The security of business IT systems has never been as important as it is today. IT underpins virtually all the activity conducted by businesses making them increasingly vulnerable to threats from hackers, viruses and even their own staff.

Effective security can mean your business is safe from malicious activity or accidental introduction of malware. Failing to secure systems, websites and manage employee usage of the internet exposes the company to great risk – risk of a damaged reputation, risk of system damage, loss of business and the cost of remedial work. This is in spite of common uses of defenses such as firewalls and intrusion detection or prevention systems.

The risk is greatly enhanced in today's business world with the advent of new technologies such as Web 2.0 and the social networking phenomenon. Furthermore, malware exploded in 2007/8 and unfortunately, this shows no signs of abating in the near future.

To reduce as much of the threat possible, organizations need to identify, analyze and report vulnerabilities in a given application. According to Gartner, 75% of attacks occur at the application level and a Forrester survey states that "people are now attacking through applications, because it is easier than through the network layer." The vulnerabilities may be present in the application due to inadvertent flaws left behind during development, security issues in the underlying environment and misconfigurations in one or more components such as the database or web server.

Security is an issue that all businesses should take very seriously and prevention is most certainly favorable to the cure. Companies must factor in the security risks with every IT related decision that is taken. This report will look at several threats and how they can be reduced through testing.

## Compliance Regulation that Enforces Increased Security Testing

There are many regulations across the globe that affect commerce, all of which present unique challenges to organisations. Security is fast becoming the focus of many of these regulatory changes, and organizations and industry bodies are working together to tackle the issues that the on-line world presents.

One industry that is enforcing its members to ensure a high degree of security is online retail – which is estimated to

generate over \$200 billion in revenues annually. Companies are being forced to ensure their networks are secure to protect themselves and their customers from potential threats.

The solution adopted to ensure security in this environment is the Payment Card Industry Data Security Standard (PCI DSS) which is specifically designed to protect customer account information of credit/debit card holders. Breach of customer information can lead to financial loss and a seriously damaged reputation for the organization. Every company that accepts credit card payments, processes credit card transactions, stores credit card data or accesses personal and sensitive data of customers is affected by the PCI DSS. This means that all businesses, regardless of size, need to understand the scope of PCI DSS, and how to implement network security processes which are compliant with PCI guidelines.

The complexities that PCI DSS compliance brings to an organization are significant. Meeting the requirements and subsequently verifying they have been met will require a good deal of planning - from business owner all the way through to IT functions. When defining a new application to support online retail, the mandatory elements of PCI DSS compliance should be built into the business requirements definition to ensure they are subsequently developed and tested against to ensure compliance.

Best practice would see the following security measures being adopted to ensure that the highest level of security is met:

- ▶ Install and maintain a firewall configuration to protect data
- ▶ Do not use vendor-supplied defaults for system passwords and other security parameters
- ▶ Encrypt transmission of cardholder data and sensitive information across public networks
- ▶ Use and regularly update anti-virus software
- ▶ Develop and maintain secure systems and applications
- ▶ Restrict access to data by business need-to-know
- ▶ Assign a unique ID to each person with computer access
- ▶ Restrict physical access to cardholder data
- ▶ Track and monitor all access to network resources and cardholder data

- ▶ Regularly test security systems and processes

These are just the main areas of risk within the on-line retail world. However, organizations, regardless of industry, should be prepared to apply increased rigor to all security aspects of their applications as new and more stringent regulatory changes are enforced.

## Changing Technologies in IT

Web 2.0 has revolutionized the internet by using existing technology in a different way to enhance communications, secure information sharing, collaboration and functionality of the web. Web 2.0 has enabled the development and evolution of web-communities and has hosted services such as social networking sites. These in particular have since exploded into societies, bringing an array of complications. Many organizations utilize such websites in order to promote their products and services or even to vet potential employees. Sites such as LinkedIn are also used for business networking purposes and many employers encourage their usage.

The complications arise from attackers. Malware targeting Web 2.0 applications is getting more diverse and harder to track and will most likely get worse as the malicious code is written with even more variants that is geared around password and identity theft. Attackers are now able to create hundreds of thousands of unique malware pieces, most of which are written with no unique signature so they can circumvent traditional signature and reputation-based, virus-detection software. Attackers will also continue to infuse legitimate websites with malicious Trojans, causing malware levels to continue to increase throughout 2009. Attackers are also getting wise to what will have the greatest effect in social networking sites, For example, they impersonate a user's contact and send a message to the user. The level of trust required for these sites means that users are likely to open a message from one of their known contacts.

Attacks can impact customers with various outcomes; the loss of their data or a corruption of systems, meaning sales cannot be processed, are two possible negative effects. The organization must put measures in place to lower the risks associated with such sites. Blocking them altogether would work but this may not be feasible. In that case, the correct firewalls must be installed and regularly updated to account for any new threats that may arise.

Furthermore, website penetration testing (this time in a Web 2.0 environment) could highlight areas of weakness. The output from testing should provide enough information to enable the organization to understand what measures it must put in place to combat the risk. If this is done objectively, a more complete covering can be ensured.

## Conclusion

The areas of risk outlined above are not exhaustive but cover very important aspects of internet security. What is crucial in minimizing risk is for development to be done to a high standard which will hopefully ensure there are fewer weaknesses in the code in the first place. Secondly, all changes in technology must be tested thoroughly to identify problem areas in order that the organization can undertake remedial work and prevent future problems.

For the best picture of the situation, testing should be as objective as possible to ensure there is 360 degree coverage eliminating as many weak spots as possible.

Breaches of security can damage a company's brand and reputation and impact on the bottom line, particularly for companies who generate the majority of their revenue through online sales. As such, business leaders need to have it high on their agenda and everything must be done to ensure your organization's safety.

*Chakri Devarakonda is Associate Manager, Security Services for AppLabs, the largest independent global provider of quality management, testing and certification services. For more information go to [AppLabs.com](http://AppLabs.com)*