SymQuest®
A KONICA MINOLTA COMPANY

SymQuest® eBook
The Layered IT Security Model

When evaluating your internal security protocol it’s helpful to use a *layered security model*.

This model begins with the internet and ends with the employee. Use this eBook as a guide to determine how well your current IT security procedures are working in your organization.

Email Filtering

The filtering of spam and virus infected email should occur outside your firewall. Not only does this reduce the amount of traffic on your internet connection, it ensures that email-based malicious code never enters your network. Additionally, you can set up your firewall to only accept email from a known source, your email filtering service.

"Email malware creation is up 26% year over year, with 317 million new pieces of malware created in 2014."
(Virtru Corporation)

Web Filtering

Employees should be prevented from accessing websites that are known malicious sites. This is not simply a matter of making sure that users are not wasting time or exhibiting questionable taste. This is about real threats to your network.

Between 200,000 to 300,000 new web sites per day host code that can result in a PC being infected with malware just by visiting the site.
(PC World)

Firewall

This is the *cyber front door* to your organization. Just like your physical front door, it should be locked down and only authorized traffic should be allowed through.

"There was an 8 percent increase in the number of browser vulnerabilities reported in 2014."
(Symantec)

Network Access Control

Only authorized devices should be allowed to connect to your network. In the case of wireless devices, access should be limited to only resources necessary to do business. For example, wireless guest access should only allow users to get to the Internet but not have any visibility to internal network resources.

> "The average cost of a corporate data breach increased 15 percent in the last year to $3.5 million."
> (Insurance Journal)

Network Security Monitoring

Just like you might have motion sensors in your office to detect suspicious movements when you are not there, you might have monitoring on your network to detect suspicious traffic. Similar to your physical security, this may be a service provided by a third party.

"North America saw a 7% decrease in financial loss attributed to security events."
(PWC)

OS Security Patches

Operating Systems (OS) are constantly being updated with security patches as vulnerabilities are discovered.

Failure to apply these patches and reboot systems regularly leaves an organization vulnerable to exploits by hackers. Once a patch is released, the entire hacker community is aware of the vulnerability.

> “92% of 100,000 analyzed incidents can be categorized by just 9 basic patterns.”
> (Verizon Enterprise)

SymQuest® A KONICA MINOLTA COMPANY

Anti-Virus/Malware Updates

New viruses are deployed every day. Your antivirus and anti-malware software needs to be kept up to date. If your AV/AM software has not been kept current, it will be unable to detect and protect your system from new viruses.

> “The number of new mobile malware samples jumped by 49% from Q4 2014 to Q1 2015.”
> (McAfee)

Application Security Patches

Similar to an OS, applications are regularly updated to address newly discovered vulnerabilities. Something as simple as opening a PDF file can put an organization at risk if the application is not up to standard.

"Attackers earned a 1,425% return on investment for exploit kit and ransomware schemes."
(Trustwave)

Employee Education

The last line of defense is the *employee*. Most major security breaches involve an employee action that enabled hackers to gain access to the system. Employees must be educated on network security best practices. Your employees should be your *human firewall*.

"34% of companies do not have a crisis response plan for a data breach or cyberattack event."
(Protiviti)

SymQuest®
A KONICA MINOLTA COMPANY

Still have questions?

Call: 1-800-374-9900

Email: info@SymQuest.com

We Are **IT** for Business

www.SymQuest.com

New York | Vermont | New Hampshire | Maine