Self-guided IT Security Audit Checklist

This self-guided security audit is offered free of charge and is designed to provide guidance to help improve corporate IT security. By evaluating the processes and technology underpinning your IT infrastructure, as well as the people employed within your organization you will expose weaknesses and better understand the risk to your data.

IT Policy

	Y/N
Do you have an IT policy all employees must agree to prior to employment?	
Do you enforce the IT policy and have the ability to easily identify infractions?	
Does the policy clearly define BYOD practices?	
Do you have a change management procedure within the IT policy?	

Employees

	Y/N
Do you train staff on how to deal with suspicious emails and data requests?	
Do you have a password policy and do you enforce it?	
Do you conduct regular interviews to measure employee satisfaction?	

Web Browsers

	Y/N
Are web browsers set to automatically update?	
If no, is this checked by a member of your IT department?	
Do you prohibit flash and other browser addons from running on your systems?	

Endpoint Security

	Y/N
Do you have a current, commercial anti-virus subscription?	
Does the anti-virus software check for updates on a regular schedule?	
Are your systems regularly scanned for virus and malware?	

Security Appliances

	Y/N
Do you use a commercial Firewall from a recognized vendor?	
Is the firewall a separate appliance or built into your router?	
Do you regularly apply firmware upgrades and patches to your firewall?	
Does the appliance have spam and malware detection and blocking capabilities?	

Infrastructure

	Y/N
Is your wireless network protected by Media Access Control address filtering (MAC)?	
Do you restrict sensitive data access and log access attempts?	
Do you encrypt sensitive data using AES 256 or higher?	
Do you encrypt all data in transit?	
Do you have an offsite back system?	
How often, if ever, do you try to recover data from your offsite backup?	
Do you have a Disaster Recovery site and a Business Continuity plan?	
Is the DR facility located at a safe distance and using a different power grid?	
Does the travel time to the DR site exceed your RTO?	

The goal of this document is to pose simple YES/NO questions that, if unaddressed, could lead to serious security risks to your organization. In just about every case you should have answered YES to the questions. If you are unable to get the answer or if you answered no, it is highly advisable you seek a consultation with an established IT Security provider.

If you have a question about this test, or require assistance in addressing any issues it uncovers; you can contact Pathway Communications by email ctogroup@pathcom.com