Quick Check for Small Business IT Security

This free questionnaire (available at www.securityviews.com under "Free Security Tools") is for average small business owner/manager (staff of 5 to 15 people), and provides a rough indication of how likely you are to be at risk, based on your business computing practices and the security safeguards you employ. This tool yields a general indicator; not a comprehensive assessment. It should not be used for assessing specific safeguards. Businesses are responsible for performing their own due diligence and risk assessments at all times when connecting computers to any networks.

No.	Information Profile	Yes	No	?
	Our business operations depend on the following types of information and systems:			
1	Regulatory information (reporting, internal auditing, etc.)			
2	Client information for fulfilling orders or services (client contact information, order descriptions and configurations, delivery statuses, trouble tickets, payment card numbers, etc.)			
3	Other Client confidential information (etc. requirements, strategy, financial info, points programs, preferences, historical info, legal info, etc.)			
4	Supplier information (parts on order, agreements, customer service program info, confidential price lists, strategic info, legal info, etc.)			
5	Partner information (strategies, negotiation details, agreements, financial info, legal info, etc.)			
6	Inventory information			
7	Internal operations information (internal trouble tickets, sales tracking info, marketing graphics and designs, product version information)			
8	Administrative information (financial history data, human resources personal and performance information, security plans and configuration info)			
9	Proprietary product designs, copyrighted digital content, original documentation, process information			
10	Specialized or specially configured computer and network hardware			
11	Software and Network media and configurations (eg. Web site software and Web page designs, ERP, order tracking software, customer service software, etc.)			
	(A) Total Information Profile Score (Total of Yes and "?" responses only)			

No.	Organizational Responsibilities	Yes	No	?
1	We have a set of security policies describing the rules for managing the protection of our IT assets including information and critical business systems.			
2	We have a top level role within the organization who is explicitly responsible for all security accountability, and all staff responsible for managing security has a reporting relationship (direct or indirect) to the individual in this role.			
3	We have a set of documentation that describes how our information assets are classified for sensitivity and protection requirements for storage and transmittal.			
4	We have documented responsibilities within the organization managing all personnel security including security screening, security awareness and security training.			
5	We have a documented risk management program in place to identify which assets are most valuable to our operations, to identify the scenarios that are most likely to cause losses, and to identify safeguards to minimize these risks.			
6	We have documented responsibilities within the organization for managing the maintenance of physical security, facilities and critical infrastructure such as power, water, fire protection, and air conditioning.			
7	We have documented responsibilities within the organization for managing the operation of all IT systems including patch updates, system security configuration and penetration testing.			

8	We have documented responsibilities within the organization for authorization of access to critical business systems, applications, networks and facilities.			
9	IF WE DEVELOP PRODUCTS, SERVICES OR UTILITIES INTERNALLY… We have documented responsibilities within the organization for managing the development and maintenance of these items according to a System Development Life Cycle.			
10	We have documented responsibilities within the organization for managing contingency planning in case of outages of our critical business systems due to malfunctions, loss of key staff, supplier failures, malicious attacks or major disasters.			
11	We have documented responsibilities for pro-active audit preparations and managing internal and external audits of our business systems.			
	(B) Total Organizational Responsibilities Score (Total of Yes responses only)			

No.	Security Practices and Culture	Yes	No	?
1	We conduct internal security audits at least once a year.			
2	We have a publicly available privacy policy that describes and limits our intended use of customer private information.			
3	We have designated computing, storage and/or handling areas for sensitive information which are secured and only accessible by people in authorized roles that need access to perform their duties.			
4	Our staff is trained and aware of our security policies to the point where they would automatically: - challenge unfamiliar or unidentified individuals on the premises, - report any breach of security policies to management - know not to click on web links or attachments within emails that are not from trusted senders			
5	We explicitly forbid software license violations, pirating or installation of unauthorized software on any of our computer systems.			
6	Our corporate connection to the internet is protected with firewall configured to hide all internal systems, except those that host servers (such as email and Web servers) in a "Public Access Zone" or Demilitarized Zone (DMZ)".			
7	We review and install security patches and updates for all our critical business systems' software including operating systems, servers and applications.			
8	Our operational data on critical systems is backed up every day, logged, labeled and stored securely, with archive copies sent off-site at least monthly.			
9	Our passwords for all users with access to critical business systems and data are strong (8 characters with a mix of upper, lower, numbers and/or special characters), and are forced to change at least every 90 days.			
10	We review our critical business systems for risks, including disasters and contingency plans at least yearly.			
11	We log all system configuration changes so that we can always identify the configuration of any computer or network system on any given date.			
	(C) Total Organizational Security Practices and Culture Score (Total of Yes responses only)			

Net Score (B ___ + C ____ = ____ - A ___ = ____)		
Score more than 12 **CONGRATULATIONS!** **Good Over-All Score** Always ensure safeguards match your exposures.	Score 8 – 12 **CAREFUL** **Medium Risk** You should formalize more of your security programs.	Score less than 8 **WARNING!** **HIGH RISK** **Seek Help ASAP!**

More security tools and resources for business and home are available at www.securityviews.com.