

Cyber Security — Best Practices Checklist

Hackers increasingly target small- and mid-sized businesses with fewer data security resources. Complete the following checklist for a quick assessment of critical cyber security best practices for your business.

Topic	Assessment
Cyber Event Preparation	<input type="checkbox"/> Written cyber security and incident response plan reviewed with all employees
Multi-Factor Authorization (MFA)	<input type="checkbox"/> Required for remote network access <input type="checkbox"/> Required for any key financial and customer information access
Employee Training	<input type="checkbox"/> Active and consistent employee cyber security awareness training
Secure Email/Encryption	<input type="checkbox"/> Using secure email when sending sensitive information, billing and/or contracts.
Money Transfer and Banking	<input type="checkbox"/> Confirms all emailed invoices against previous statements and contacts accounts payable to confirm changes <input type="checkbox"/> Does not accept any emailed changes to bank or routing numbers without verbal confirmation
Data Backup	<input type="checkbox"/> Off network backup of key financial and customer data <input type="checkbox"/> Minimum once per week, preferably every day
Firewall	<input type="checkbox"/> Using network firewall to prevent malicious network traffic
Passwords	<input type="checkbox"/> Using password manager for any computer network access
Website Security	<input type="checkbox"/> "Bookmarks" commonly used financial (i.e. banking, credit card) and vendor websites <input type="checkbox"/> Employees recognize/use only Hypertext Transfer Protocol Secure (HTTPS) sites
Information Security	<input type="checkbox"/> Limits gathering of unnecessary customer information (e.g. SSN) or keeping customer credit card information <input type="checkbox"/> Limits employee access to financial/customer information
Wireless Security	<input type="checkbox"/> Using WPA2 encryption <input type="checkbox"/> Not using company name for network ID (SSID) <input type="checkbox"/> Wireless router set to automatically take software updates
Software Security	<input type="checkbox"/> Using anti-virus software, spam/phishing filters <input type="checkbox"/> Computers set to automatically take updates
Physical Security	<input type="checkbox"/> Sensitive documents, thumb drives and backups stored in secure filing cabinet/safe <input type="checkbox"/> Encryption enabled on mobile devices <input type="checkbox"/> Remote "wipe" of mobile devices enabled

Sample Form

F70-954.5 Ed. 05-22

This sample form is provided as a courtesy. The material is intended to be general in nature and is not intended to establish programs or policies specific to your business. Since each business situation is unique, this sample form should be edited to meet your specialized circumstances and needs. This form should not be considered tax, legal or other expert advice. This form is not intended to comply with any state, federal or local laws or regulations. Use of this form may help reduce the risk of loss, but should not be construed as eliminating any or all risk of loss nor is it an exhaustive list of all risk exposures. Obtain the advice of independent legal or business advisors in developing these forms and procedures to meet the specialized circumstances and laws applicable to your business.