MIS

Cybersecurity Assessment

Your cybersecurity plan should focus on three areas to ensure that your organization's systems are not compromised and that your data or money does not wind up in the wrong hands - people, process and technology.

People

Do your employees understand the importance of protecting proprietary information and the consequences of a data breach? Are they properly trained in cybersecurity best practices to prevent criminals from gaining access to your network, accounts and applications?

Process

Do you have the proper processes in place that offer a clear blueprint of how your company's sensitive data should be handled, what steps are to be taken to prevent a data breach, and what to do in the event of a cyber incident?

Technology

Are you or your current IT company utilizing the latest tools and technology to adhere to your industry's compliance standards and to shore up your network and reduce the endpoint security risks of your organization?

Is your business protected? Take our 5-10 minute assessment to help determine your organization's risk score and where your business could improve.

Instructions: The following is a list of cybersecurity protocols that every business should adhere to for optimal safety. Please put a number in the space provided that best fits how well your organization *currently* is performing in these areas.

0 - NOT AT ALL
1 - SOMEWHAT
2 - MODERATELY
3 - EXCELLING IN THIS AREA

PEOPLE	RATING
Are you providing information about computer and network security to your staff?	
Are employees taught to be alert to possible security breaches?	
Do you offer security awareness training to your employees?	
Do you restrict employees from visiting certain websites?	
Are visitors escorted into and out of controlled areas?	
Does management regularly review lists of individuals with physical access to sensitive facilities or electronic access to information systems?	
Do you cancel access to systems and facilities for former employees, contractors and vendors immediately after termination?	
Have you communicated with your staff protocols for a cybersecurity incident?	
Have you identified who will speak to the press/public in the case of an emergency or an incident?	
Add up your total people score	

PROCESS	RATING
Does your company have an Acceptable Use Policy that covers computers, laptops, mobile phones and tablets?	
Does your Acceptable Use Policy clearly outline what is considered "business confidential"?	
Does your Acceptable Use Policy clearly outline unauthorized copying of copyrighted materials?	
Does your Acceptable Use Policy clearly outline revealing your account passwords to others?	
Does your Acceptable Use Policy clearly outline circumventing user authentication or security of any host, network or account?	
Does your Acceptable Use Policy clearly outline introducing honeypots, honeynets or similar technologies on the company network?	
Does your Acceptable Use Policy clearly outline what to do in the case of theft or loss of a device?	
Does your Acceptable Use Policy clearly outline monitoring and surveillance by the company?	
Does your Acceptable Use Policy clearly outline company rights to audit?	
Does your Acceptable Use Policy clearly outline providing information about or lists of company employees to parties outside of the company?	
Does your Acceptable Use Policy clearly outline email and communication activities?	
Does your Acceptable Use Policy clearly outline blogging and Social Media?	
Do you have policies and procedures in place that address allowing authorized and limiting unauthorized physical access to electronic information systems and the facilities in which they are housed?	

PROCESS	RATING
Is access to your computing area controlled (single point, reception or security desk, sign-in/sign-out log, temporary visitor badges)?	
Do you have procedures for protecting data during equipment repairs?	
Is there a process for creating retrievable backup and archival copies of critical information?	
Does your company have a process for the disposal of old hardware and equipment and rendering it unusable and inaccessible?	
Do your policies for disposing of old computer equipment protect against loss of data (e.g. by reading old disks and hard drives)?	
Do you have a current business continuity plan?	
Do you have a current risk assessment?	
Do you have a procedure for notifying authorities in the case of a disaster or security incident?	
Do you review and revise your security documents, such as policies, standards, procedures and guidelines on a regular basis?	
Do you audit your processes and procedures for compliance with established policies and standards?	
Do you have a clearly defined mobile device policy with security protocols?	
Do you have a documented process in the event of a cybersecurity threat?	
Do you have policies regarding remote access defined?	
Do you classify your data, identifying sensitive data versus non-sensitive?	
Are computer screens automatically locked after 10 minutes idle?	
Does your company have a cybersecurity insurance policy?	

PROCESS	RATING
Do you have a policy for identifying the retention of information (both hard and soft copies)?	
Do you have procedures in place to deal with credit card information?	
Is there a process for creating retrievable backup and archival copies of critical information?	
Do you test your disaster plans on a regular basis?	
Add up your total process score	

TECHNOLOGY	RATING
Are anti-malware, next-generation anti-virus, advanced threat detection solutions installed on your network?	
Does your IT provider conduct regular software patches and updates?	
Is the most valuable or sensitive data encrypted?	
Do you have secure encrypted email for sensitive data?	
Do you use spam filtering software?	
Do you conduct regular security audits and penetration testing?	
Do you have external penetration tests performed on a regular basis?	
Does your organization have and enforce the use of a password manager and demand users use complex passwords?	
Do you use multi-factor authentication to access company data?	
Do you control or lockdown third-party applications such as Dropbox?	
Do you have an enterprise-class firewall installed that is secured and regularly updated and monitored?	
Do you ensure systematic review of log files and backup logs to make sure there are no errors?	

TECHNOLOGY	RATING
Do you have Secure Sockets Layer (SSL) in place when using the internet for secure data transfers?	
Add up your total technology score	

Add up your scores below:

PEOPLE	
PROCESS	
TECHNOLOGY	
TOTAL	

115-168 = Your business is excelling at cybersecurity.
56-114 = Your business is moderately excelling at cybersecurity.
20-55 = Your business is somewhat excelling at cybersecurity.
0-19 = Your business is not excelling at cybersecurity.

Whether you scored a 168 or a 0 on your cybersecurity performance, you must have an IT provider that can help you navigate your cybersecurity and grow your business. Imagine if you could give every single box a 3? Our team would love to help you get there!

Reach out to us at info@mis-solutions.com or give our team of technology experts a call at 678-745-5109.


MIS
Make IT Possible