✔ Be Ready ✔ Plan Ahead ✔ Take Action ✔ Follow Up

YOUR CYBERSECURITY CHECKLIST

Technology has transformed the way we all do business for the better. However, to keep your data and business from being at risk, you must ensure your tech is secure and continuously monitored. We're providing this detailed checklist as a reference tool to help you verify that comprehensive cybersecurity and physical security policies are in place throughout your organization.

Cybersecurity is defined as a system of technologies, processes, and practices designed to protect your computers, networks, applications, and data from attack, damage, or unauthorized access.

IDENTIFICATION PROCEDURES

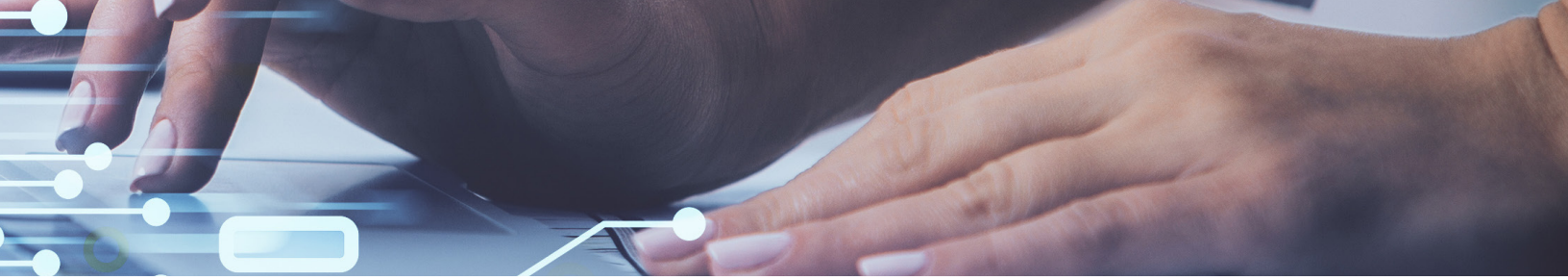
	YES	NO
• Do all your staff members have photo ID badges?		
• Do they wear them at all time when in your facility?		
• Do you provide temporary ID badges for visitors?		
• Do you check the credentials of visitors?		
• Is a policy in place for conducting background checks for employees and visitors?		
• Can you cut off access to employees and visitors if necessary?		

PERSONAL & PHYSICAL SECURITY

	YES	NO
• Do you have procedures in place to prevent unauthorized physical access to computers and other electronic information systems?		
• Do you have solutions in place to prevent physical access to your secure areas, such as door locks, access control systems, security offices, or video surveillance monitoring?		
• Do you have security desks, and sign-in/sign-out logs for users accessing these areas?		
• Do you physically escort visitors out of secure areas?		
• Can you ensure users always log out of their computers when leaving them?		
• Are all computers set to lock automatically after 10 minutes if left idle?		
• Can you remotely wipe computers, laptops, and mobile devices that are lost or stolen?		
• Is there a policy in place to protect data during equipment repairs?		
• Do you have security policies in place for all of your computers, laptops, tablets, and smartphones?		
• Do you have a “Bring Your Own Device” policy in place for employee mobile devices?		
• Do you have emergency evacuation plans in place for employees?		
• Do all employees have emergency shelter-in-place kits for emergencies where they can’t leave your facility? (canned food and a can opener, bottled water, a blanket, prescription medicines, sanitary wipes, a garbage bag with ties and toilet paper for personal sanitation)		
• Do key employees know how to seal off designated areas in your facility if necessary?		

ACCESS CONTROL POLICIES

	YES	NO
• Do you adhere to the NIST Digital Guidelines?		
• Do only authorized personnel have password access to computer devices?		
• Do you require users adopt secure password standards (NIST) and then enforce them?		
• Are passwords updated every three months?		



• Do administrators have separate accounts for network management?		
• Do you use MFA everywhere you can?		
• Do you enforce MFA on remote access email and sensitive documents?		
• Do you use secure methods (VPN) for remote systems access?		
• Do you maintain a "zero-trust" security culture?		

DATA PRIVACY POLICIES

	YES	NO
• Is your data stored in a secure offsite facility?		
• Is all confidential data encrypted?		
• Do you have procedures in place to identify and secure the location of confidential information – whether as digital or hard copies?		
• Do you have procedures in place to identify and secure the location of personal private information?		
• Do you continually create retrievable backup and archival copies of critical information?		
• Do you have procedures in place for shredding and securely disposing of paper documents?		
• Do you lock your shredding and recycling bins?		
• Do you have policies in place for secure disposal of electronic/computer equipment?		
• Do you have policies in place for secure disposal of electronic media such as thumb drives, tapes, CDs and DVDs, etc.?		
• Do you have procedures in place to regularly assess IT compliance with required regulations (HIPAA, PCI, FINRA, GDPR, CCPA, etc.)?		
• Do you conduct regular reviews of users with physical access to protected facilities or electronic access to information technology systems?		
• Do you deploy systems in a hardened/secure state?		
• Do you have a vulnerability management system that detects and fixes vulnerabilities on all devices (workstations, network equipment, server equipment, etc.)?		
• Do you have a third-party company that runs an annual penetration test?		
• Do you enforce a "Clear Desk and Screen" policy to keep all confidential information hidden?		

BUSINESS CONTINUITY & DISASTER RECOVERY

	YES	NO
• Do you have an up-to-date business continuity and disaster recovery plan in place?		
• Do you create retrievable backups of critical data?		
• Are your backups stored offline in a secure cloud and are those backups immutable from ransomware or a similar event?		
• Does your backup, continuity, and recovery plan include a method for accessing critical passwords for equipment, systems, and servers when needed?		
• Does your backup, continuity, and recovery plan include a method for accessing encryption keys in an emergency?		

	YES	NO
• Do you have an up-to-date crisis communications plan?		
• Does your crisis communications plan identify who should be contacted, how to contact them, contact information, and who initiates the contacting?		
• Do you have a PR representative who will communicate to the press and community in an emergency?		
• Does your crisis communications plan detail how employees can contact their family members?		
• Have you identified recovery time objectives for each system, and tested for achievability?		
• Do you regularly test your business continuity, disaster, and crisis communications plans?		
• Do you receive alerts if backups are turned off?		
• Do you receive alerts when there is a change in backup size or retention status?		
• Do you regularly review backup settings to know if anyone has maliciously adjusted them?		
• Do you regularly review your cyber insurance policy to be sure it provides the right coverage?		

CYBERSECURITY TRAINING

	YES	NO
• Do you provide staff training from an IT expert on cybersecurity?		
• Do you provide this training on a regular basis?		
• Does your staff know how to recognize phishing attempts in emails?		
• Does your staff know how to recognize phishing attempts that arrive via text, social media, or phone calls?		
• Are your employees trained on reporting phishing emails to the security team?		
• Are your employees being taught about using secure passwords?		
• Are your employees trained to identify and protect classified data, as well as hard copies of documents and removable media?		
• Is your staff trained on secure management of credit card data (PCI standards) and private personal information?		

COMPLIANCE REVIEW

	YES	NO
• Do you regularly review and update your cybersecurity requirements, strategies, plans, and practices?		
• Do you conduct regular audits of your security requirements, strategies, plans, and practices?		
• Are you testing your backup and disaster recovery plans regularly?		
• Do you conduct regular reviews of who in your organization has access to sensitive information and data?		
• Do you have an inventory of your authorized devices and software?		
• Do you regularly test all your systems for vulnerabilities?		
• Are you following the best practices established by the Center for Internet Security (CIS) in their CIS Controls?		

For each question where you answered "No," you should implement activities to correct the deficits or vulnerabilities to the security of your data, facility, or personnel. Unless you take action, the ability for your business to thrive/survive will be negatively impacted. Be sure to also follow up and reassess by completing this survey again in six months' time. After that, we advise that you continue to review these questions on an annual basis.

CYBERSECURITY THREAT/ RISK ASSESSMENT

A cybersecurity threat is a person or a thing that accidentally triggers or intentionally exploits a vulnerability or weakness within your organization. A number of threats may be present within you network or operating environment. Threats can come from natural and environmental elements as well as from people.

Natural Threats:

- Storm/Flood Damage
- Fire
- Lightning Strikes
- Hurricanes/Tornadoes
- Pandemic

Environmental Threats:

- Power Outages
- Chemical Spills
- Pollution

Human Threats:

- Computer Abuse
- Terrorism
- Sabotage
- Vandalism
- Fraud
- Errors/Negligence
- Falsified Data
- Unauthorized Access
- System Tampering
- Civil Unrest

CALCULATE YOUR RISK

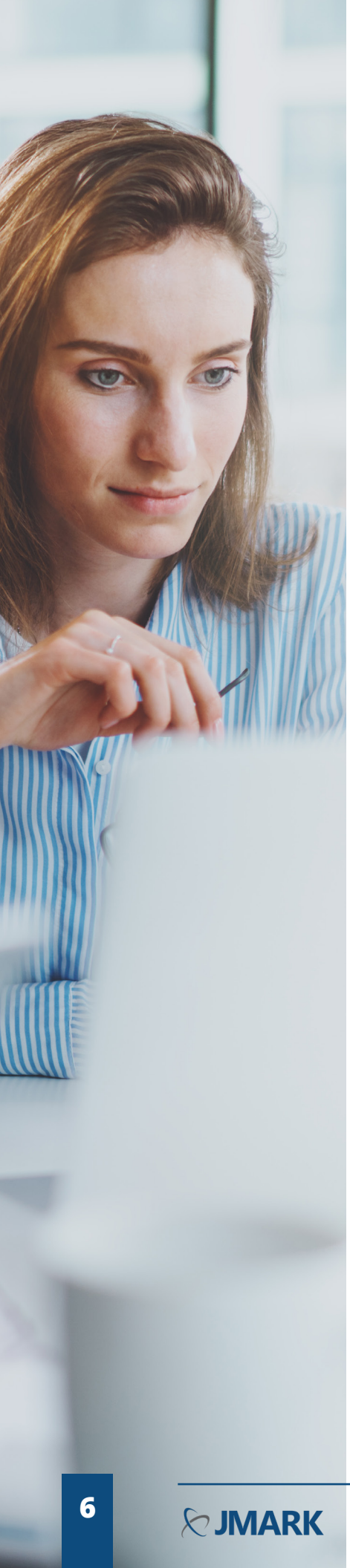
"Risk is a combination of the likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury of ill health that can be caused by the event or exposure(s)." (OHSAS 18001:2017) Risk is part of every business environment, but unless you can keep risk in check, it can grow. Losses can be avoided by assessing the potential for these threats and vulnerabilities and determining the specific risks your organization faces.

Risk = Impact x Likelihood

Use this numeric rating scale to determine your potential risk.

Impact (0-6) Likelihood (0-5)

When assessing the impact, consider the value of the assets that are at risk, what it will cost to replace them, and their importance. The things that affect likelihood include threat capability, frequency of occurrence, and the effectiveness of the countermeasures available to you.



IMPACT SCALE

- The impact is negligible.
- The effect is minor. Most operations are not affected.
- Your operations shut down for a period of time, resulting in financial loss. Customer confidence is slightly affected.
- You experience a loss of operations resulting in a significant impact on public/customer confidence.
- The effects are devastating. Systems shut down for extended periods of time. Systems must be rebuilt and data must be replaced.
- The effect is ruinous. Critical systems go offline for extended periods of time. Data gets lost or is corrupted beyond repair. The health and safety of employees is affected.

LIKELIHOOD SCALE

- Not likely to occur.
- Not likely to occur more than once a year.
- This is likely to occur once a year.
- This is likely to occur once a month.
- This is likely to occur each week.
- This is likely to occur on a daily basis.

People can significantly impair the ability of your organization to operate effectively.

PEOPLE	DESCRIPTION
Stakeholders	Employees, owners, stock holders, etc.
Contractors	Cleaning company, maintenance contractors, technical support, computer repair services, etc.
Former Employees	Retired, resigned, or were fired
Unauthorized Users	Cybercriminals, terrorists, and intruders

Use the following to assess your risk level for each threat/vulnerability.

SCORE	RISK LEVEL	RISK RESULT
21-30	High Risk	• Major loss of assets, data, or information resources. • Completely disrupts operations for a week or more. • Destroys your reputation.
11-20	Medium Risk	• Substantial loss of assets, data, or information resources. • Disrupts operations for a few days. Damages your reputation.
1-10	Low Risk	• There is a minor loss of assets or information resources. • Slightly affects the organization's operation (for less than one day). Minor loss to reputation.

ASSESS THREATS AND VULNERABILITIES

Enter your Impact and Likelihood numbers to assess your threat level.

HUMAN THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
Human Error			
• Accidental deletion, modification, disclosure, or wrong classification of information.			
• Negligence: lack of security awareness or conduct, inadequate documentation, uninformed.			
• Workload: lack of adequate staff, and employees feel stressed.			
• Users knowingly reveal security weaknesses to criminals.			
• Improper system configuration.			
• Inadequate security policies.			
• Security policies are not enforced.			
• Security analysis incorrect or inadequate.			
Corruption			
• Fraud, theft, sellling of conficential information.			
Social Engineering Attacks			
• Criminals use email or phone calls and impersonate an employee to gain confidential information.			
• Criminals execute ransomware and malware programs due to employees inadvertently letting them into your network.			
Abuse of Trust			
• Long-term or high-level employees take advantage of relaxed security policies.			

GENERAL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Unauthorized use of computers.			
• Mistakenly combining test and production data or environments.			
• Use of unauthorized software or hardware.			
• Design errors in operating system (using a system not designed to be highly secure).			
• Protocol design errors: certain protocols were not designed to be highly secure. Protocol weaknesses in TCP/IP can result in:			
• Source routing, DNS spoofing, TCP sequence guessing, unauthorized access.			
• Time bombs: software programmed to damage a system on a certain date.			
• Hijacked sessions and authentication session/transaction replay, data is changed or copied during transmission.			
• Denial of service due to ICMP bombing, TCP-SYN flooding, large PING packets, etc.			
• Logic bomb: software programmed to damage a system under certain conditions.			
• Viruses in programs, documents, email attachments.			

ACCESS CONTROL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Password hacking.			
• External access to password files, and packet sniffers to access data.			
• External attack programs gain unauthorized access to the network (backdoors).			
• Internal attack programs gain unauthorized access to the network.			
• The existence of unsecured maintenance modes via developer backdoors.			
• Bugs in network software that leave security holes.			
• Unauthorized physical access to your system.			

REFUSAL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Those receiving confidential information refuse to acknowledge receipt.			
• Those sending confidentinal information refuse to acknowledge the source.			

LEGAL/REGULATORY THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Failure to comply with legal/regulatory requirements, such as protecting confidentiality of employee or customer data.			
• Your organization is liable for actions by employees or internal users who use your network to conduct unlawful activities (such as money laundering, pornography, gambling, etc.)			
• Your organization is liable for damages because employees or other internal users hack other sites.			

NATURAL DISASTERS & HUMAN THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Your productivity and services are halted due to disasters: fire, smoke, water, earthquake, storms (hurricanes, tornadoes), power outages, etc.			
• Your productivity and services are interrupted due to minor disasters of short duration.			
• Major human-caused disasters such as war, terrorism, bombs, civil disturbances, chemical spills, radiological accidents, etc. halt or interrupt your productivity and services.			
• Defective hardware, cabling, communications systems, or other equipment cause interruptions in productivity or services.			

CYBERCRIME THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Likelihood)
• Misuse of routing protocols that confuse and mislead systems.			
• Server overloading that shuts down systems.			
• Email bombing by bad actors.			
• Downloading or receipt of malware.			
• Sabotage with deliberate damage to data or information processing functions.			
• Destruction of physical network interface devices, cables, etc.			
• Destruction of computing devices, media, etc.			
• Destruction of devices and media with electromagnetic radiation weapons.			
• Deliberately overloading electricity or shutting it off.			
• Deploying viruses and/or worms to delete critical systems files.			
• Overloading data circuits with a large volume of frivolous requests.			
• Employees being fooled by phishing emails.			

REMEDIATION ACTIVITIES

After assessing, reviewing, and rating potential threats and vulnerabilities, you should determine what actions you can take to reduce your risk. This means employing security controls, and/or increasing the strength of existing controls. Always balance the cost of doing this against the expected security benefit and risk reduction. Most remediation efforts and actions focus on the high-risk threats and vulnerabilites first.

The following table lists remediation activities you can take. They are prioritized based on their effectiveness.

RANK	REMEDIATION ACTIVITY	COST	BENEFIT	RISK
1	Establish security policies, practices, and procedures. This is very important during times of change.	LOW	HIGH	HIGH
2	Develop and enforce a globally-accepted password strategy.	LOW	HIGH	HIGH
3	List vulnerabilities in order of high to low risk.	LOW	HIGH	HIGH
4	Facilitate discussions to improve processes and communications.	LOW	HIGH	HIGH
5	Set up and follow router configuration security standards and best practices.	LOW	HIGH	HIGH
6	Harden servers on the network.	LOW	HIGH	HIGH
7	Incorporate worker termination activities with HR and IT policies.	LOW TO MODERATE	HIGH	HIGH
8	Conduct new-hire orientation, security awareness training, and annual "refresher" courses for all employees.	LOW TO MODERATE	HIGH	HIGH
9	Utilize multi-tier architecture and defense of depth in the design of your internet perimeter and enterprise architecture.	LOW TO MODERATE	HIGH	HIGH
10	Convert to a centralized and integrated model of operations management that incorporates centralized logging, event correlation, and alerting.	LOW TO MODERATE	HIGH	HIGH
11	Install an intrustion detection system.	MODERATE	HIGH	HIGH
12	Deploy encryption on mobile devices to protect the confidentiality and integrity of data.	MODERATE TO EXPENSIVE	HIGH	HIGH
13	Employ data classification to define security levels.	MODERATE TO EXPENSIVE	HIGH	HIGH
14	Conduct vulnerability assesments on a regular basis.	MODERATE TO EXPENSIVE	HIGH	HIGH
15	Designate email as mission-critical.	LOW	MODERATE	MEDIUM
16	Ensure adequate security staffing for the ISO Security Group.	EXPENSIVE	HIGH	HIGH
17	Implement Computer Security Incident Response Team (CSIRT) capabilities.	MODERATE TO EXPENSIVE	HIGH	HIGH

As you can see, securing your organization's technology is a complex task. Yet with the help of an expert IT partner, you can rest assured your company is safe. For more information, contact JMARK at 844-44-JMARK or email JMARKIT@JMARK.com. Our team has the knowledge and skill to secure your business and keep your company safe.