YOUR CYBERSECURITY CHECKLIST

Technology has transformed the way you do business for the better. However, you must ensure it's always secure and monitored continually, or your data and business will be at risk. The same goes for the security and protection of your staff in the event of an emergency. We're providing this detailed checklist as a reference tool for you to verify that adequate cybersecurity and physical security policies are in place.

Logicspeak℠

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

IDENTIFICATION PROCEDURES	YES	NO
• Do all your staff members all have Photo-ID Badges?	☐	☐
• Do they wear them at all times 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 officers, 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 automatically lock after 10 minutes if left idle?	☐	☐
• Can you remotely wipe computers and laptops that are lost or stolen?	☐	☐
• Are all modems in Auto-Answer OFF mode when not in use?	☐	☐
• 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 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, and sanitary wipes, 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?	☐	☐

PASSWORD 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?	☐	☐

DATA PRIVACY POLICIES

	YES	NO
• Is your data is 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 both in digital and 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, etc.)	☐	☐
• Do you conduct regular reviews of users with physical access to protected facilities or electronic access to information technology systems?	☐	☐

BUSINESS CONTINUITY & DISASTER RECOVERY

	YES	NO
• Do you have an up-to-date business continuity and disaster recovery plan in place?	☐	☐
• Can you create retrievable backups of critical data?	☐	☐
• Are your backups stored offline in a secure cloud?	☐	☐
• Do you have an up-to-date crisis communications plan?	☐	☐
• Does your crisis communication plan identify who should be contacted, how to contact them, contact information, and who initiates the contacting? (e.g., a phone tree)	☐	☐

BUSINESS CONTINUITY & DISASTER RECOVERY	YES	NO
• Do you have a PR representative who will communicate to the press/community in an emergency?	☐	☐
• Does your crisis communications plan detail how employees can contact their family members?	☐	☐
• Do you regularly test your business continuity, disaster and crisis communications plans?	☐	☐

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?	☐	☐
• 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 personal private 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?	☐	☐

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 do so 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 your network or operating environment. Threats can be from natural and environmental elements and well as from people.

Natural Threats:
- Storm/Flood Damage
- Fire
- Lightning Strikes
- Hurricanes/Tornados

Environmental Threats:
- Power Outages
- Chemical Spills
- Pollution

Human Threats:
- Computer Abuse
- Terrorism
- Sabotage
- Vandalism
- Fraud
- Errors/Negligence
- Falsified Data
- Unauthorized Access
- System Tampering

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 or ill health that can be caused by the event or exposure(s)." (OHSAS 18001:2017) Risk is a part of your business environment. Unless you can keep it in check, it can grow. Losses can be avoided by assessing the potential for these threats and vulnerabilities, you can determine the potential 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 effect likelihood include: threat capability, frequency of occurrence, and the effectiveness of the countermeasures available to you.

IMPACT SCALE	LIKELIHOOD SCALE
• The impact is negligible	Not likely to occur
• The effect is minor. Most operations aren't affected.	Not likely to occur more than once a year
• Your operations shut down for a period of time resulting in financial loss. Customer confidence is slightly affected.	This is likely to occur once a year
• You experience a loss of operations resulting in a significant impact on pubic/customer confidence.	This is likely to occur once a month.
• The effects are devastating. Systems shut down for extended periods of time. Systems must be rebuilt and data must be replaced.	This is likely to occur each week.
• 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.	This is likely to occur on a daily basis.

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

PEOPLE	DESCRIPTION
• Stakeholders	1. Employees, owners, stock holders, etc.
• Contractors	2. Cleaning company, maintenance contractors, technical support, and computer repair services, etc.
• Former employees	3. Retired, resigned, or were fired.
• Unauthorized users	4. Cybercriminals, terrorists, and intruders

Use the following to assess the 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's 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 Probability Numbers to Assess Your Threat Level.

HUMAN THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
1. 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 unknowingly reveal security weaknesses to criminals			
• Improper system configuration			
• Inadequate security policies			
• Security policies aren't enforced.			
• Security analysis incorrect or inadequate			

HUMAN THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
2. Corruption:			
Fraud, theft, selling of confidential information			
3. Social Engineering Attacks			
• Criminals use email or phone calls and impersonate an employee to gain confidential information.			
• Criminals execute Trojan Horse and malware programs due to employees inadvertently letting them into your network.			
4. Abuse of Trust			

GENERAL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• Unauthorized use of computers			
• Mistakenly combining test and production data or environments			
• Use of unauthorized software or hardware			
• Design errors in operating system (aren't 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, e-mail attachments			

IDENTIFICATION AUTHORIZATION THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• Attack programs disguised as normal ones			
• Attack hardware disguised as normal commercial hardware			
• Criminals pretending to be authorized users or customers			
• Internal attackers pretend to be valid users or customers			
• Criminals disguised as helpdesk personnel			

PRIVACY THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• Eavesdroppers			
• Electromagnetic eavesdropping / Van Eck radiation			
• Phone/fax eavesdropping with listening devices, inductive sensors, or by breaking into public telephone exchanges			
• Unauthorized discovery of sensitive data via unknown internal networks			
• Illegal redirection of email or other traffic			
• Eavesdropping with radio signals			
• Trash bin theft to obtain confidential documents.			

INTEGRITY / ACCURACY THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• Malicious, deliberate destruction of data processing functions by criminals			
• Malicious, deliberate destruction of data processing functions those inside the organization			
• Deliberate revision of information			

ACCESS CONTROL THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• 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			
• Modems that open an uncontrollable extension of the internal network			
• Bugs in network software that leave security holes. This threat is increasing with more complex software programs.			
• Unauthorized physical access to system			

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

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

SERVICE THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• When your productivity and services are halted due to natural disasters, fire, smoke, water, earthquake, storms/hurricanes/ tornadoes, power outages, etc.			
• When your productivity and services are interrupted due to minor natural disasters, of short duration.			
• Where major human-caused disasters such as war, terrorism, bombs, civil disturbances, chemical spills, radiological accidents, etc., halt or interrupt your productivity and services.			
• When defective hardware, cabling, communications system or other equipment cause interruptions in productivity or services.			
• Where equipment failure from airborne dust, electromagnetic interference, or static electricity interrupts your productivity or services.			

DENIAL OF SERVICE THREATS	Impact (0-6)	Probability (0-5)	Score (Impact x Probability)
• 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.			

REMEDIATION ACTIVITIES

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

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. Conduct new-hire orientation, security awareness training and annual "refresher" courses for all employees.	Low to Moderate	High	High
8	Utilize N-Tier Architecture and Defense in Depth into the design of the Internet perimeter and enterprise architecture.	Low to Moderate	High	High
9	Convert to a centralized and integrated model of operations management that incorporates centralized logging, event correlation, and alerting.	Low to Moderate	High	High
10	Install an Intrusion-Detection System.	Moderate	High	High
11	Deploy encryption on mobile devices to protect the confidentiality and integrity of data.	Moderate to Expensive	High	High