SMB CYBERSECURITY RISK ANALYSIS

QUESTIONNAIRE

STREAMSCAN

www.streamscan.ai

1-877-208-9040

GETTING STARTED

Follow our step-by-step cybersecurity risk analysis process to understand where your risks are and where you should prioritize your security investments. If you don't have an experienced cybersecurity expert on your team, make sure you engage one to accompany your team on this exercise.

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Security Governance Framework		
Does your organization have an approved and communicated cybersecurity governance framework? If so, can you provide a list of the security policies?		
If you have a security governance framework, do you review it at least once a year?		
If you have a security governance framework, is it actively communicated to the organization?		
Information Security Organization		
Are information security roles and responsibilities formally defined, documented and communicated in your organization?		
Security Governance Framework • Yes • Yes, dedicated department/service • Yes, but integrated into another department/service • No		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Security Risk Management Policy		
Do you have a documented security risk assessment process, including risk acceptance criteria and risk assessment criteria?		
Do you have a documented risk assessment process including risk response options (remediation, risk transfer, risk acceptance, etc.)?		
If you have a security risk management plan, does it include the roles and responsibilities of the stakeholders in the risk management process as well as the timelines for implementing the treatment measures?		
Network Access Control		
Do you have an identity and access management policy for your IT environment?		
Do you have a documented and communicated internal password policy? If so, please provide the rules.		
Do you have a process that covers the entire life cycle of user access management in your network (creating, modifying, deleting, deactivating access, managing employee departures, etc.)?		
Do you apply the "Least Privilege Principle" when granting access to users on your network? This principle states that users should be given only the strict minimum rights necessary to do their job.		
Do you apply the "Need to Know" principle when providing access to your network (only those who need access to information in order to do their job have access)?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Network Access Control		
Are initial passwords and other secret authentications provided by secure means?		
Do your users have only access to the networks and services for which they are specifically authorized?		
Do the designated owners of your information assets periodically verify all access rights to the assets?		
Do you periodically review access to your network?		
Are there clear rules in place for users on how to protect passwords and other authentication information?		
Are the access rights of all employees and subcontractors deleted immediately upon termination?		
Remote Access Security and Surface of Attack Limitation		
What type of remote access solution do you use: RDP, VPN, etc.?		
Is multi-factor authentication (MFA) required for remote access?		
When attempting to log in remotely, do accounts lock up after multiple failed login attempts?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Remote Access Security and Surface of Attack Limitation		
If so, after how many failed remote access attempts will the accounts lock? (e.g. 5, 10, etc.)		
Do you have technology that alerts you in case of unauthorized access attempts from outside (e.g.: log management tool - SIEM, intrusion detection system - IDS, etc.)? If yes, which?		
Email Security		
Do you have a security policy for use of email?		
Is your email solution hosted internally or externally (e.g. O365 in the Cloud)?		
Is multi-factor authentication (MFA) required for access to your mailboxes?		
When attempting to log in remotely, do accounts lock up after a certain number of failed login attempts?		
If applicable, after how many failed remote access attempts will the accounts lock?		
Does your email solution have features to block or quarantine incoming malicious emails?		
Does your email solution have features to detect failed access attempts (e.g., list of at-risk users, users logged on in unlikely locations)?		
Protection Against Phishing		
Are your employees regularly educated about the risks of phishing?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Protection Against Phishing		
If so, how often do you educate your employees?		
Have you educated your employees at least 1 time since March 2020?		
Data Backup		
Is your data backed up regularly?		
If so, how often do you make backups?		
Do you have a recent backup copy of data online and another copy offline?		
Do you maintain an offsite data backup?		
Is your backup solution isolated from the servers whose data you are backing up?		
Do you do regular data recovery tests?		
If so, how often do you perform data recovery tests?		
Vulnerability Management		
Do you have a formal policy for managing security vulnerabilities?		
Do you have a person or team formally designated to take charge of collecting information on vulnerabilities (security vulnerability watch)?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Vulnerability Management		
How do you currently identify security vulnerabilities in your network? • Periodic penetration tests • Regular vulnerability scans • Security patch management process • Other, please specify.		
Are the vulnerabilities reported and promptly resolved according to their level of severity?		
Do you restrict software installation by users on your computer network?		
Do you audit network security regularly?		
If you regularly audit your network security, how often do you do it?		
Do you do regular penetration tests in your network and/or applications?		
If you do regular penetration tests, how often do you do them?		
Safe Internet Browsing		
Do you use a web browsing filtering solution to ensure that employees do not browse unauthorized or malicious websites?		
Are your employees regularly trained to understand the risks related to Internet browsing? If so, how often?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Remote Work Safety (COVID-19)		
When telecommuting, do your employees have to connect to your network to use the Internet (e.g. VPN)?		
Do employees use their own computers to remotely connect to your network?		
If employees connect via their own computer, do you take steps to ensure that they have a working antivirus on their computer?		
Do you provide a corporate antivirus to employees who access your network via their personal computer?		
Have you done any training on the security risks of telecommuting?		
Security Incident Response Plan		
Do you have a cyber attack response policy or plan?		
Are security incident management roles and responsibilities clearly defined and communicated?		
Do you have established procedures for reporting security events and incidents?		
Are all information security events reported in a timely manner?		
Do your employees have an obligation to report security breaches that they see or identify?		
Are identified vulnerabilities promptly resolved according to their level of severity?		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Security Incident Response Plan		
Are security incidents analyzed in order to gain knowledge about vulnerabilities that allowed them to occur (root cause analysis)?		
Do you perform regular incident response tests? If so, how often?		
Understanding Your Security Risks		
What do you think are the biggest security risks for your organization? • Internal attacks • Hacking attempts • Viruses transmitted via email • Malware • Phishing • Incorrect configuration • Uncontrolled personal mobile devices (BOYD) • Online extortion • Other, please specify.		
Knowledge of Security Incidents		
Has your organization experienced any security incidents in the past 24 months?		
If yes, list the cases involved and the number of incidents that occurred : • Theft or unauthorized access to personal information • Virus attacks • Hacker attacks • Malicious tools (ransomware, etc.) • Loss of assets (theft or loss of computers, external storage media) • Leakage or unauthorized disclosure of sensitive information • Other, please specify.		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Business Continuity Management		
Do you have a business continuity and disaster recovery plan?		
Do you have a disaster recovery environment for your critical IT infrastructure?		
If you do regular continuity testing and disaster recovery? How often do you do it?		
Privacy and Compliance Management		
Do you have a privacy or data protection policy?		
Do you periodically check your compliance with applicable security policies and standards?		
Is the security of your information systems regularly reviewed for compliance with your information security policies?		
Network Perimeter Defense		
What security measure(s) does your organization have in place to protect against cyber attacks? • Antivirus on all workstations and servers • Endpoint protection technology (EDR) installed on all servers and workstations • Firewalls • Anti-spam/spyware/anti-phishing solutions • Intrusion detection systems or security breaches/intrusion prevention systems/security breaches (IPS/IDS/NDR) • Security event management solutions (SIEM) • Data loss prevention systems (DLP) • File and data encryption • Other, please specify.		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Network Perimeter Defense		
Have you ever performed penetration testing within your organization? • Yes, by an external • Yes, by an internal team • No		
Protection of Confidential Data		
Do you hold confidential information? If so, what is the nature of this data? • Personally identifiable information (PII) • Credit card data • Business secrets and intellectual property (IP) • Other, please specify.		
If you have confidential data, do you keep an accurate inventory of that data?		
Do you share confidential data with third parties (subcontractors, etc.)?		
Do you have your partners sign a confidentiality agreement (NDA) before sharing confidential information with them?		
Do you have procedures that ensure the respect of intellectual property rights, in particular, the use of licensed software?		
Do you currently have a data retention policy that clearly states how long you will retain data?		
How do you currently protect the confidential data you hold? • Data encryption • Access control (limiting the number of people who have access to this data) • Strong or multi-factor authentication (MFA) • Other, please enumerate.		

SPECIFIC AREAS OF RISK	STATUS Yes/No	COMMENTS
Protection of Confidential Data		
Do you know who in your organization has access to confidential data (personal information, etc.)?		
Is the personal information you hold protected as required by laws and regulations?		
Do you have a technology to detect and prevent data exfiltration attempts (or information leakage)?		

TAKE CHARGE OF YOUR CYBERSECURITY TODAY

How Can We Help ?

If your organization needs help to conduct a risk analysis, a security audit, develop a security plan or implement a Managed Detection and Response solution, or if you just have questions about cybersecurity, get in touch with us at: info@streamscan.ai

About StreamScan

Network security is every bit as important to small and medium-sized companies as it is to multinationals. The fact is 1 out of 4 Canadian companies of all sizes will have their networks compromised each year. Our solutions are designed and priced specifically for small to medium-sized organizations.

StreamScan's Managed Detection and Response service leverages our AI-powered network monitoring CDS technology to provide enterprise-level protection at a price that will make sense to you. To learn more about StreamScan, visit our website at: www.streamscan.ai