LOFFLER

CYBERSECURITY CHECKLIST

Implementing the tips on this checklist can help you evaluate and prioritize your approach to cybersecurity based on your organization's unique needs. These are some of the most common cybersecurity topics we discuss with our clients.

SCAN TO DOWNLOAD

01. IMPLEMENT MULTI-FACTOR AUTHENTICATION (MFA)

MFA requires users to provide two or more verification methods to gain access to accounts and applications. Start with your email and VPN.

Implement Multi-Factor Authentication (MFA) for all critical and public-facing systems.

Done □ In Progress □ Not Started □

02. SECURE YOUR WINDOWS REMOTE DESKTOP SERVICES (RDP)

RDP allows users to control a remote Windows machine as if they were working on it locally.

Ensure that Windows Remote Desktop Services (RDP Protocol) are not exposed through your firewall in an insecure fashion.

Done □ In Progress □ Not Started □

03. SECURITY ASSESSMENTS & VULNERABILITY SCANNING

Security assessments will give you a hollistic view of your cybersecurity posture. This is a great place to start finding weaknesses in your security controls.

Perform an annual security assessment and an annual vulnerability scan to determine risks that are specific to your organization.

Done □ In Progress □ Not Started □

04. CREATE A SECURITY STEERING COMMITTEE

A team dedicated to security provides clear direction and visible support for security iniatives. This will help develop a cyber-aware culture at your organization.

Create a security steering committee to drive continous improvement. Use the data gathered from annual assessments to address any unique cybersecurity risks to your organization.

Done □ In Progress □ Not Started □

05. MAINTAIN FULL DATA BACKUPS

Proper data backups can be the difference between a complete loss and a complete recovery in the event of a ransomware attack.

Ensure backups are complete, perform test restores regularly and have an 'air-gapped' and encrypted copy of the backups that cannot be deleted by an attacker.

Done □ In Progress □ Not Started □

06. DETECT & PREVENT MALICIOUS SOFTWARE

Endpoint Detection & Response (EDR) tools help you readily identify, detect and prevent cyber threats.

Implement an Endpoint Detection & Response solution to protect your laptops, desktops and servers beyond what a traditional antivirus can achieve.

Done □ In Progress □ Not Started □

07. EDUCATE END-USERS

The greatest risks to information security are your end-users. Around 88% of security incidents are caused by human error.

Train employees on your organization's cybersecurity policies, security best practices, and email security, and test their knowledge with simulated phishing emails on a regular basis.

Done □ In Progress □ Not Started □

08. CREATE AN INCIDENT RESPONSE PLAN

An Incident Response Plan (IR Plan) acts as a playbook for your organization to follow in the event of a cyber attack or suspected compromise.

Create an Incident Response Plan. Test and review your plan annually.

Done □ In Progress □ Not Started □

09. MANAGE YOUR HARDWARE & SOFTWARE LIFECYCLE

Outdated devices and software introduce vulnerabilites that attackers can exploit to gain access to your network.

Manage the lifecycle of hardware and software to ensure you don't have unsupported systems that introduce security risks.

Done □ In Progress □ Not Started □

10. ENABLE CENTRALIZED LOGGING & ALERTING

Collecting and analyzing vast amounts of logging data can overwhelm staff. Centralized event log management lets you filter for the most significant security data.

Enable centralized and managed logging analysis and alerting for all systems, software, cloud services and firewalls.

Done □ In Progress □ Not Started □

11. IMPLEMENT A VULNERABILITY MANAGEMENT PROCESS

Create a process to manage and maintain system updates and validate that the updates were implemented sucessfully. Confirm that the updates were able to harden system configurations.

Implement a vulnerability management process that ensures all critical security patches are applied in a timely fashion and periodically validated.

Done □ In Progress □ Not Started □

12. CREATE CLEAR & CONCISE CYBERSECURITY POLICIES

A cybersecurity policy helps your employees to understand their role in protecting the technology and information assets of your business.

Implement cybersecurity policies that employees will be able to understand and follow without causing end-user frustration.

Done □ In Progress □ Not Started □

13. USE A PASSWORD MANAGER

Password managers store your login information in an encrypted database with a master password – you only have to remember one password for every login!

Administer a password manager to support your written password policy and access control policy.

Done □ In Progress □ Not Started □

14. INVEST IN A CYBER INSURANCE POLICY

Any organization that uses and stores data will benefit from cyber insurance. Check all the boxes on this list and you'll be in a good position to obtain a cybersecurity insurance policy.

Review your cyber insurance policy and make sure you have the right coverage for the current work environment and cyber-threat landscape.

Done □ In Progress □ Not Started □

NOTES: