NEXT PERIMETER

CYBERSECURITY CHECKLIST

NextPerimeter.com // 888-286-4816

MORE CYBERATTACKS ARE TARGETING SMBS

Cyberattacks targeting SMBs are on the rise. Small and medium-sized businesses will be a bigger and bigger target for cybercriminals in the 2020s. In fact, 76% of SMBs in the U.S. reported a cyberattack in 2019, compared to only 55% in 2018, a 32% increase, according to the "Ponemon 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses" report.

Phishing attacks continue to be the most common type of attack, with data loss including sensitive employee and customer data being the most common result of such an attack

This checklist will help you confirm you're protecting yourself and your customers by reducing your attack surface and improving your ability to prevent, detect, and respond to attacks.

NOTE: These recommendations cannot cover every aspect of your security needs. Your approach to cybersecurity will depend largely on your IT environment (network, systems, size, framework, etc.), and some advice may not be appropriate for your company.

Do what's sensible, take a layered approach, and also bear in mind, when implementing new controls, it's always a good idea to test them first to stay clear of unplanned interruption.

SAFETY AND SECURITY

IS NOT

A ONE-SIZE-FITS-ALL APPROACH.

RESTRICT ACCESS ACROSS YOUR NETWORK

Today's cyberattacks are becoming more sophisticated, and malicious actors are leveraging automated malware and human-operated campaigns against businesses large and small. These campaigns exhibit extensive knowledge of systems administration, network security configurations, software vulnerabilities, use reconnaissance, and they adapt to what they discover in a compromised network. To protect your business against this, you need to establish barriers around your users and assets

- [ ] Actively inventory all network assets* and classify them by risk. *Resources: Walkthrough*
- [ ] Use unique, case-sensitive passwords combining letters, numbers, and symbol. We recommend using a business grade password manager like *LastPass*
- [ ] Enable multi-factor authentication. whenever possible. *Resources: Office 365*
- [ ] Refrain from using default usernames. (admin, administrator, default, user, etc.)
- [ ] Use the principle of least-privilege by limiting user access and account privileges to the bare minimum required to perform necessary job functions.
- [ ] Create buffers between different tiers of privileged access. *Resources: Walkthrough*
- [ ] Avoid the use of admin accounts for non-admin functions
- [ ] Apply "least privilege" to service accounts for specific applications. *Resources: Tips to avoid service account misuse; walkthrough of using Group Managed Service Accounts*
- [ ] Use unique local admin passwords. *Resources: Microsoft's Local Administrator Password Solution (LAPS)*
- [ ] Remove end users from local admin group.
- [ ] Block lateral movement between workstations.

73%

OF EXECUTIVES HAVE LITTLE OR NO INSIGHT INTO WHAT PHYSICAL DEVICES ARE CONNECTED TO THEIR BUSINESS NETWORK.

Ponemon Institute
2019 Global State of Cybersecurity in Small and Medium-Sized Businesses

NEED HELP SECURING YOUR NETWORK?

RECEIVE A FREE NETWORK SECURITY ASSESSMENT FROM A CERTIFIED NETWORK SECURITY SPECIALIST.

SECURING REMOTE MANAGEMENT TOOLS

Not only are remote access capabilities critical to your business, there are also few things an attacker would love to hijack more.

- [ ] Restrict access to remote management tools and accounts.
- [ ] Use strong, unique passwords and multi-factor authentication
- [ ] Limit what remote accounts have access to.
- [ ] Don't log in to workstations with domain administrator accounts.
- [ ] Keep remote management software up to date.
- [ ] Enable centralized logging, monitoring and alerting for remote access sessions.

SECURING REMOTE DESKTOP (RDP/RDS)

Securing remote desktops (RDPs) may be a basic practice, but failure to do so continues to be one of the leading causes of compromise.

- [ ] Don't expose RDP (or any internal resources) to the internet unless absolutely necessary.
- [ ] Use port scanners to identify RDPs (and other ports and services) exposed to the internet. *Resources: ShieldsUP, Nmap, Shodan*
- [ ] Identify systems that have been compromised with RDP backdoors. *Resources: Tools available here or here*
- [ ] Disable RDP on machines that don't need it.

29%

OF USERS WHO OPEN A PHISHING EMAIL ENGAGE WITH IT.

Proofpoint
2020 State of the Phish

- [ ] Remove local admin account access to RDP and create a restricted user group in the Group Policy Management Console instead.
- [ ] Implement an account lockout policy to prevent successful brute-force attacks. *Resources: Microsoft recommendations*
- [ ] Log off disconnected and idle sessions.
- [ ] Restrict RDP access using firewalls, RD Gateways, and VPNs. *Resources: How to restrict RDP access to whitelisted IP addresses; more info on RD Gateways*
- [ ] Leave network level authentication (NLA) enabled. *Resources: How to check your Group Policy settings to confirm NLA is enabled*
- [ ] Change the default listening port (TCP 3389) *Resources: Walkthrough*

PROTECT YOUR USERS AND ENDPOINTS

The human element is the most vulnerable part of your network. Let's review best practices you can implement to protect users and secure devices.

- [ ] Use endpoint security software with antivirus (AV) with machine-learning and/or behavioral analysis in addition to or in place of signature matching.
- [ ] Keep endpoint systems and software up to date by **automating patch management.**
- [ ] Develop a standard operating procedure (SOP) for auditing your firewall policies and critical endpoints.
- [ ] Utilize DNS filtering to protect against known malicious websites.
- [ ] Utilize a spam filtering service for active email protection, such as Microsoft ATP

- [ ] Set up DMARC, SPF and DKIM to protect your domain from being spoofed. *Resources: Walkthrough; free DMARC monitoring and reporting tool*

- [ ] Provide security awareness training to employees to help them spot malicious emails and websites. Resources: US Department of Health & Human Services Cybersecurity Awareness Training.

- [ ] Utilize a reliable backup and disaster recovery solution following the 3-2-1 backup rule.

- [ ] Test backups regularly to ensure recovery.

PROTECT YOUR USERS AND ENDPOINTS

Cybercriminals know many SMBs don't have the technical expertise to harden systems appropriately. These "tricks" allow them to bypass defenses and evade detection by impersonating legitimate administration activity. Here are steps you can take to mitigate "out-of-the-box" vulnerabilities.

- [ ] Guard against credential dumping by limiting or disabling credential caching. *Resource: Walkthrough for Windows 10 and Server 2016; walkthrough for older systems*

- [ ] Disable or restrict PowerShell with Constrained Language Mode and AppLocker. *Resources: Walkthrough*

- [ ] Restrict the launch of script files. *Resources: Walkthrough for Windows 10; walkthrough for older systems*

- [ ] Use AppLocker to restrict applications link. *Resource: AppLocker design guide*

- [ ] "living-off-the-land" binaries (LOLbins) or restrict them from making outbound requests. *Resources: List of LOLbins (start with certutil, mshta, and regsvr32); walkthrough for using Windows Firewall to restrict programs from making outbound requests*

- [ ] Utilize the Windows Firewall to block malicious remote access and lateral movement. *Resources: Walkthrough*

- [ ] Restrict or monitor Windows Management Instrumentation (WMI) Resources: Examples of defensive WMI event subscriptions; walkthrough for setting a fixed port for WMI (and blocking it if remote WMI isn't necessary)

- [ ] Use highest user account control (UAC) enforcement levels whenever feasible (including enabling admin approval mode for built-in admin account). Resources: Walkthrough for Windows 10; walkthrough for older systems

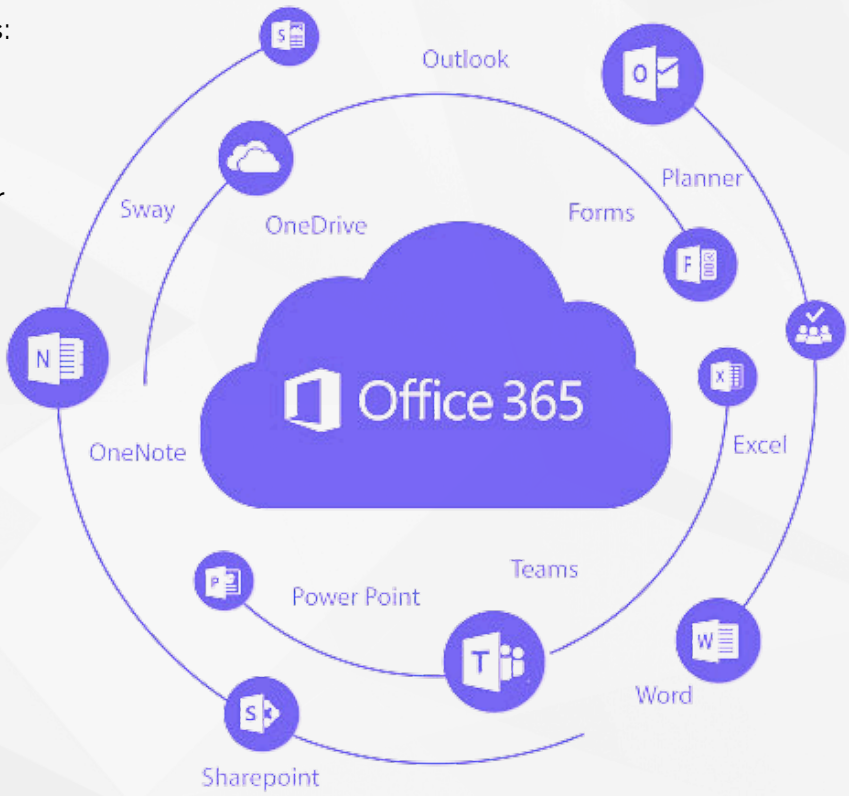
SECURING MICROSOFT OFFICE

Microsoft Office documents and Windows applications are the most common and successful delivery methods used by cybercriminals to deliver malicious payloads. Here's what you need to do to mitigate these threats:

- [ ] Disable or restrict macros. Resources: Walkthrough for Office 2016; Group Policy Administrative Template files (ADMX/ ADML)

- [ ] Disable or restrict Object Linking and Embedding (OLE). Resources: Walkthrough for blocking activation of OLE packages via registry changes; walkthrough for blocking activation of OLE / COM components in Office 365 via registry change; walkthrough for disabling data connections and automatic update of Workbook Links via the Trust Center.

- [ ] Disable Dynamic Data Exchange (DDE). Resources: Walkthrough for ensuring applications are properly secured when processing DDE fields; walkthrough for disabling via the Trust Center



DETECT & RESPOND TO SECURITY INCIDENTS

It's not enough to only focus on preventing cyberattacks. Inevitably, most business networks will experience some form of compromise, whether it's caused by an unintentional risky click on a phishing email or a disgruntled employee saving intellectual property. It's not a matter of IF but WHEN. For this reason, you need to focus on the whole cybersecurity lifecycle by ensuring you have the right people, technologies, and processes in place to effectively detect, contain, investigate, and remediate threats swiftly.

THE AVERAGE TIME TO IDENTIFY A BREACH IN 2019 WAS 206 DAYS, AND THE AVERAGE TIME TO CONTAIN A BREACH WAS 73 DAYS, A TOTAL OF 279 DAYS. THIS REPRESENTS A 4.9% INCREASE OVER THE 2018 BREACH LIFECYCLE OF 266 DAYS.

IBM
2019 Cost of a Data Breach Report

MONITORING

Real-time monitoring and alerting is key to identifying potential security incidents as quickly as possible. The trick is balancing visibility with prioritization and noise reduction. Otherwise, you risk suffering alert fatigue and feeling like you're drinking from a fire hose.

- [ ] Establish a network performance baseline so you can identify anomalies
- [ ] Use your RMM and/or SIEM to **configure centralized network and endpoint monitoring.**
- [ ] **Create standard monitoring and alert settings** you can apply across workstations, servers, etc.
- [ ] **Prioritize alerts by establishing classifications** based on severity (critical, high, low) and create notification policies for each.

COMPREHENSIVE SECURITY DOESN'T NEED TO BE EXPENSIVE.

PROTECT YOUR BUSINESS WITH ADVANCED IT SECURITY SOLUTIONS FROM NEXT PERIMETER AT A FRACTION OF THE COST IT WOULD REQUIRE TO HIRE JUST ONE SECURITY PROFESSIONAL, AND RECEIVE UNLIMITED IT SUPPORT.

- [ ] Develop standard operating procedures for addressing most critical and most common alerts.
- [ ] Reduce noise by eliminating alerts that lack severity and aren't actionable.
- [ ] Monitor key Windows event IDs that could indicate malicious activity. Resources: Lists here and here
- [ ] Consider utilizing an endpoint detection and response (EDR) solution.
- [ ] Enable and configure the right system logs to assist in your own or outsourced digital forensics and incident response (DFIR). Resources: Cheat sheets for Windows
- [ ] Store logs in a central, isolated location.
- [ ] Determine if you need to outsource management for all or some of the above to a managed detection and response (MDR) provider.

CREATING AN INCIDENT-RESPONSE PLAN

Phew! By now you have seriously enhanced your organization's security posture. Response times are everything when it comes to security incidents, and having clear procedures in place will help your team reactive decisively. Let's review best practices for creating an incident-response plan.

- [ ] Define what constitutes a security incident.
- [ ] Establish roles, responsibilities and procedures for responding to incidents, including disaster recovery.
- [ ] Identify escalation options should require more extensive expert response and recovery than you can provide.
- [ ] Have a plan for communicating internally, with customers, the authorities, and the public (if necessary).
- [ ] Understand compliance requirements regarding incident disclosure and reporting.
- [ ] Understand compliance requirements regarding incident disclosure and reporting. Resources: HIPAA Breach Notification Rule; GDPR data breach notifications FAQ.
- [ ] Run fire drills

WHAT SETS US APART?

It All Starts in the Cloud

Your .com is what ties your business to the web, allowing you to get your email and collaborate online. Whether you're using Google Workspace or Microsoft 365, **Next Perimeter** has you covered. Your team can leverage our certified experts for matters concerning your email deliverability, DNS records, licensing concierge, and more.

Your Team and Workstations are Fully Covered

When your team logs into your corporate environment today, what types of protections exist? **Next Perimeter**, by default, deploys endpoint security and hardware monitoring to every workstation that we manage, ensuring productivity is at an all-time high. Your team will enjoy unlimited round-the-clock support for everyday issues ranging from authentication to hiccups with their equipment.

Battle-Tested SOPs

Whether we will handle all of your IT, or collaborate with an internal team, our procedures have been perfected against millions of business scenarios. Our system has been trained to adapt to each customer as their organizations evolve.

Future-Proofed for Compliance

We know you want your cybersecurity to be reliable, predictable, functional, and cost-effective - that's why we've simplified cyber so it's back-of-mind. By signing up for Essentials, you've created a predictable path toward future compliance needs as our agents can fulfill virtually all requirements they might ask for with simple per-user/device pricing.

NEXT PERIMETER

Let's Work Together

Phone
888-286-4816

Mail
sales@nextperimeter.com

Website
NextPerimeter.com

Get More Done Confidently and Securely with Next Perimeter

Find out how Next Perimeter makes it easier for SMBs to protect themselves and their customers with these services:

- Vulnerability and penetration testing
- Managed endpoint security
- Advanced email security
- Cybersecurity awareness training
- SIEMS - incident response
- HIPAA and PCI DSS Compliance Audits