VONAHI SECURITY

WHITE PAPER

Top 10 Cyber Security Best Practices for SMBs

Table of Contents

OVERVIEW

As small and mid-sized businesses (SMBs) embrace new technological developments like the rise of artificial intelligence (AI), cloud computing, and the internet of things (IoT), they often overlook the security implications of digital transformation. This leaves many organizations vulnerable to cyber theft, scams, extortion, and countless other cyber crimes. As a result, **two in three** SMBs suffered a security breach in the last year and cyber attacks are becoming increasingly sophisticated, targeted, and damaging. With the average cost per incident exceeding $380,000 as it is, a single security breach can be detrimental to a small firm. It is, therefore, vital that SMBs begin prioritizing cyber security. The following best practices can give your organization a head start in terms of both security and compliance.

Two in three SMBs suffered cyberattacks and data breaches in the past year.

Source: 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses by Keeper Security and Ponemon Institute

0x01

SECURITY AWARENESS TRAINING

SMBs need to address what is usually the weakest link in an organization's cyber defenses: the people working there. Clever threat actors don't hack machines; they hack people, using various forms of psychological manipulation known as social engineering. Social engineering attacks like **phishing** are incredibly successful, forming the first stage in 93% of cyber attacks that result in a security breach. The reason? Employees don't know enough about social engineering attacks to recognize one when they are at the receiving end.

WHAT SMBs SHOULD DO

- Provide general cyber security awareness training for all employees once or twice a year, and individual training for all new members of staff. A 2018 **report** shows that, while most mid-sized firms do provide at least some sort of cyber security training, very small organizations usually do not.
- **Regularly conduct phishing** and other social engineering experiments to measure the effectiveness of cyber security awareness training. According to a 2018 **survey**, two in every three SMBs put themselves at risk by not testing their staff.

0x02

PASSWORD MANAGEMENT[1]

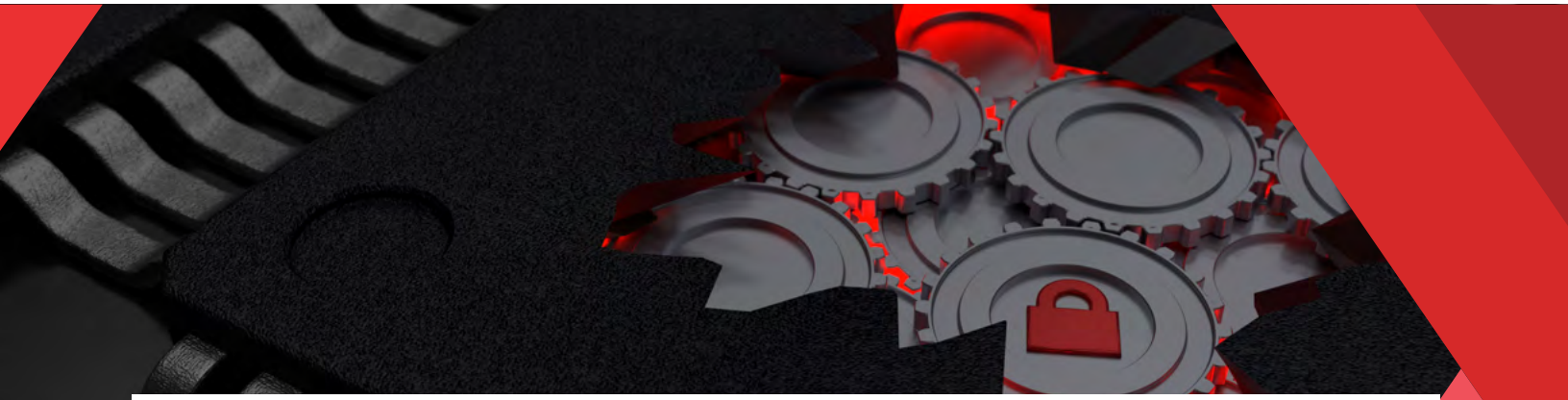
Poor password management is putting many SMBs at risk. In 2018, **two out of five** SMBs were hit by a cyber attack because threat actors cracked employee passwords. In order to prevent this from happening, organizations should implement a proper password policy.

WHAT SMBs SHOULD DO

- Enforce password length: passwords should be between 12 and 64 characters.
- Enforce password changes after a security breach, or when a breach is suspected.
- Implement **multi-factor authentication (MFA)**. This protection adds another layer of security in the event your password is stolen. Most apps have this option.
- Encourage the use of password managers.
- Implement a company-wide password policy prohibiting:
  - Passwords that have already been compromised in a data breach.
  - The use of repetitive characters (5555aaaa) and sequences (ABCD1234).
  - The use of dictionary words.
  - The use of words specific to the context in which the password is used (e.g. the username, the name of the service, or words closely related to these).
  - Password sharing – It is estimated that around **20%** of small business owners and staff members share their password with one or more colleagues.
  - Employees should never share passwords. They should have a dedicated login account.
  - Password reuse – Industry research shows that **one in four** staff members use one and the same password for all their accounts.

Useful Resource // **NIST SP 800-63B**

[1]Various online services, including **Have I Been Pwned**, allow users to check whether their email account has been compromised in a data breach.



0x03

PATCH MANAGEMENT

One major risk to organizations stems from security flaws in operating systems, applications, and hardware components that threat actors can exploit to break into computer systems. A 2018 report showed that unpatched vulnerabilities accounted for 57% of security breaches affecting large organizations and this percentage is unlikely to be lower for smaller firms. In order to reduce their risk, SMBs need to implement a patch management strategy ensuring that security fixes for discovered vulnerabilities are installed in an organized, timely manner. This is easier said than done, since the overwhelming number of vulnerabilities published each year (over 17,000 in 2018) can make it hard to see the forest for the trees.

WHAT SMBs SHOULD DO

- Make an inventory of all hardware devices and software applications on their network and keep it up-to-date by tracking changes.
- Get a **decent patch management solution** to help monitor, test, and deploy security fixes. Testing is essential to make sure that new patches will not cause systems to break down upon installation.
- Prioritize fixes for critical flaws.
- Automate the otherwise overwhelming patching process in a responsible manner by carefully configuring patch management software.
- Ensure that patch management software include the patching of both native and third-party applications.

0x04

CONFIGURATION MANAGEMENT

To prevent failures in system performance and security, SMBs also need to make sure that their operating systems, software applications, and hardware devices are set up correctly. Configuration management not only improves network security, but the use of baselines (see below) also makes it easier for organizations to detect security breaches. This is crucial because the damage resulting from a breach can be minimized through prompt identification and containment.

WHAT SMBs SHOULD DO

- Use the inventory of hardware devices and software applications mentioned above under "patch management" to figure out which solutions need to be configured.
- Get a quality **configuration management tool**.
- Set configuration baselines for relevant devices and applications. It is advised to follow established benchmarks for individual solutions, if available (see below). This process involves "hardening", i.e. maximizing security by optimizing settings and eliminating unnecessary functions.
- Test and update baselines to account for network changes and to improve performance and security.
- Monitor system performance and investigate significant deviations from baselines to see if they indicate malicious activity, performance failures, or legitimate changes that require adjustment of baselines.

Useful Resource // **NIST SP 800-128** // **CIS BENCHMARKS**

0x05

INGRESS & EGRESS FILTERING

Careful consideration should be placed on which traffic should be allowed to and from the organization's network. When data is transmitted across a network, it is broken down into small units called packets that contain information about the source IP address, the destination IP address, and the contents they are carrying to the destination, where they will be reassembled. In order to block malicious incoming traffic and illegitimate outgoing data transfers, SMBs need to implement ingress and egress filtering.

Ingress filtering vs egress filtering

- Ingress filtering is the scanning and allowing or blocking of packets coming into the company network from the public Internet. The main purpose of ingress filtering is to prevent unnecessary access to network ports and services that should be restricted only to trusted networks.
- Egress filtering works the same way, but applies to outgoing traffic. Egress filtering helps safeguard against data leaks, content filtering, and cybertheft by preventing (sensitive) information from leaving the network through unapproved network ports.

WHAT SMBs SHOULD DO

- Set up access control lists (ACLs) on all firewalls to filter incoming and outgoing Internet traffic as well as internal traffic, i.e. packets traveling between network segments.
- Permit traffic to only important ports and services, such as HTTP (80/tcp) and HTTPS (443/tcp). Access to other ports should be restricted.
- Consider implementing a web content filter to ensure that computer systems are only browsing to sites that comply with a list of website categories defined by the network administrator.

0x06

BACKUP & DISASTER RECOVERY (BDR)

Even a mature cyber security program will not and simply cannot provide complete security for a variety of reasons, including the fact that any computer program and any hardware device may at any time be vulnerable to attacks that have not been publicly disclosed. Because threat actors are constantly probing computer systems in hopes of finding new security flaws to exploit, organizations can never be 100% sure that their devices and data are safe. This makes it crucial for SMBs to implement a solid backup and disaster recovery strategy that will enable them to recover their systems in case a ransomware attack or another cyber security disaster leaves them without access to important data and/or applications.

WHAT SMBs SHOULD DO

- Make sure the backups are located off-site and not connected to your network, so if your business is hacked, the threat actors won't have access to them. These backups should also be password protected and encrypted.
- Make an inventory of all important data and software (including operating systems).
- Assess the threats to all items in the inventory and calculate the actual risk of different disasters, while taking into account all security measures in place.
- Develop a backup and recovery strategy that accounts for all relevant disasters.
- Create a written plan based on the above.
- Get a comprehensive BDR solution to help with backup and recovery.
- Implement a BDR plan, test it regularly, and keep it up-to-date.

0x07

ENDPOINT DETECTION & RESPONSE (EDR)

Internet-connected devices such as desktops, laptops, mobile devices, printers, and point of sale (POS) terminals require extra protection, as each of these endpoints can be targeted by a hacker to gain access to the network with potentially devastating consequences. According to industry research, a single compromised endpoint will cost an SMB $763 on average. For effective protection against advanced threats, organizations need to supplement traditional endpoint security in the form of an anti-malware suite with an endpoint detection & response (EDR) solution.

Benefits of EDR

Whereas traditional anti-malware suites merely detect and mitigate fairly straight-forward, known threats on individual endpoints, EDR solutions provide more comprehensive protection by:

- Monitoring of activity on individual endpoints and analysis of aggregated data from across the entire network.
- Detection and investigation and reporting of malicious activity based on:
  - Reputation – detection of blacklisted applications, users, processes and devices.
  - Behavior – detection of complex patterns of activity that indicate sophisticated malicious behavior (e.g., fileless malware).
- Immediate and effective neutralization of detected threats.
- Supporting both automated detection and response, as well as manual intervention by an administrator.

WHAT SMBs SHOULD DO

- **Get a quality EDR solution.** There are numerous paid options available.

0x08

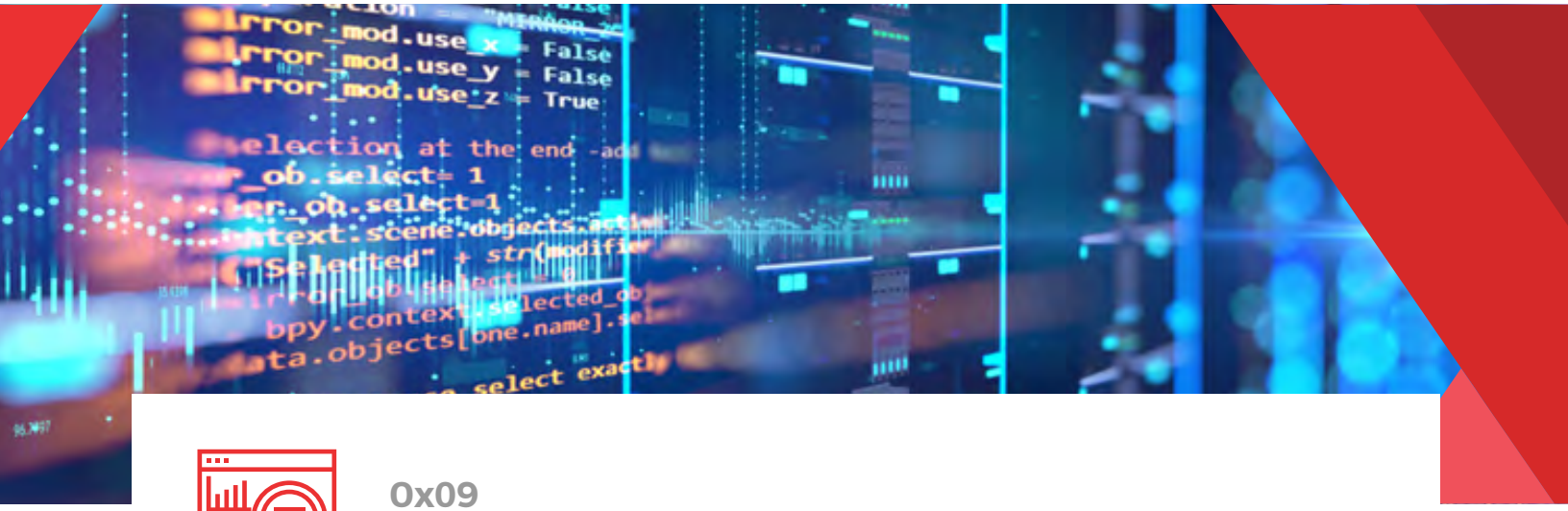
NETWORK SEGMENTATION

SMBs should also divide up their network into smaller, separate elements, or subnets, to make sure that, if a threat actor manages to gain a foothold in the company network, they will have a hard time moving across the network and accessing valuable assets. This can be achieved through network segmentation.

WHAT SMBs SHOULD DO

- Create and configure virtual local area networks (VLANs). A VLAN is a virtual subnetwork, which means that physical separation of network infrastructure is not necessary. This allows companies to split their network up into logical elements, such as:
  - Subnets for general business functions accessible to all relevant employees.
  - Subnets for highly sensitive data/processes accessible to privileged staff only.
  - Subnets for point-of-sale (POS) environments.
  - Subnets for third-parties (e.g. vendors, business partners), such as an extranet.
  - A subnet for guests.
- Install and configure firewalls for each subnet to prevent unauthorized communication between network segments (see section 0x5 on ingress and egress filtering).
- Consider implementing a zero trust network infrastructure for extra security. Zero trust involves the isolation of network elements like devices and applications through micro-segmentation.

Useful Resource // **PCI DSS** // **ISO/IEC 27002** // **FINDING GAPS IN YOUR NETWORK SEGMENTATION USING LEPRECHAUN**



0x09

LOG MANAGEMENT

Another way for organizations to monitor what happens on their network is by keeping track of logs, which are files containing information regarding relevant events occurring on a system. Logs are produced by security software, operating systems, and other applications. Proper log management is essential for SMBs, as it can enable them to spot malicious and otherwise problematic activity on their systems.

WHAT SMBs SHOULD DO

- Install a log management solution – This is software designed to help with the collection, analysis, storage, and disposal of enormous amounts of log files.
- Turn on logging for all systems that may produce relevant information. Logging activity should be configured so that only important events are recorded, such as authentication failures.
- Store or dispose logs depending on the information they contain. Superficial information, such as a simple error message, may be useful to collect, but not to store. However, data providing deeper insights into important network activity should be kept for further analysis and possibly archived afterward.
- Analyze and address logs – A log management solution can detect and report known patterns of problematic or malicious activity and exceptional deviations from baselines defining regular activity. Reported events should be investigated to address issues and malicious activity.

Useful Resource // **NIST SP 800-92**

0x0A

NETWORK INTRUSION DETECTION & PREVENTION SYSTEM

In addition to filtering incoming and outgoing traffic, organizations need to put a solution in place to monitor what happens on their network, so that malicious activity does not go unnoticed. This is where an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) can make all the difference.

IDS vs IPS

An IDS is a somewhat more basic solution than an IPS. The former will only monitor traffic and alert a system administrator when it notices something suspicious, while the latter will also try to block any malicious activity it registers. An IDS or IPS solution should monitor traffic coming into the network, as well as traffic within the network, and must be carefully configured to avoid it raising many false positives. Both solutions can come in the form of a hardware device that needs to be physically connected to the network, or as a software program.

WHAT SMBs SHOULD DO

- **Get a quality IDS and/or IPS solution.** Smaller firms with limited security budgets – unfortunately, this phrase is practically synonymous with "SMBs" – can consider one of the software-based IDS solutions **available for free.**

BONUS SECTION (PAID SERVICES)

BASIC SECURITY

IMPLEMENTING CYBER SECURITY ON A $5K ANNUAL BUDGET

1. User Awareness Training (free/cheap training content available)

Educate your employees about cyber threats! If employees are not trained, then the risk they will get infected increases dramatically. Develop a mindset where they're looking out for suspicious emails and practicing how to avoid becoming a target. There are many security awareness solutions, including free ones like **https://wizer-training.com** that include 1-min animated training videos.

2. Health Check & Vulnerability Assessment

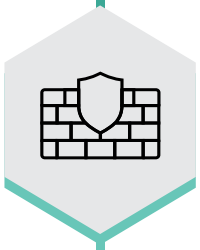
This should be performed once a quarter and will basically check for any security vulnerabilities with applications or computers on the network that may allow hackers in. Hackers are also using vulnerability scanning techniques on your network to try to get in, so you better be ahead of them.

3. Internet Access Constraints

Depending on the type of business, try to limit access to the internet as much as possible. For example, do not allow employees to browse the web from your POS terminal. If hacked, then all your customer credit card information could be stolen. Some businesses limit employees from accessing the internet and have dedicated a standalone Chromebook laptop for accessing the payroll and accounting systems.

4. Computer Access Control

Lock down your computers - make sure employees have limited permission, for example they should not have permissions to install apps. This is also known as the principle of least privilege, where users only have the necessary access to perform their job functions. Also, verify that only the absolutely necessary applications are installed. Unnecessarily exposed services can expose computers to additional attack vectors.



5. Firewall

Obtain a network firewall and configure it properly. This will limit who can access your business from the outside and will control how data exits your business. If you are using Windows based computers, then enable Windows Firewall on all workstations - blocking incoming connections. Other operating systems including Mac OS X and Linux come with built-in host-based firewalls as well.

6. Inventory and Patch Management

This will allow you to know what is installed and ensures all apps, computers, and POS systems are updated and patched to the latest versions. Unpatched computers and apps are open doors for hackers... so make sure they are always up-to-date.

7. Termination policies

Make sure terminated employees don't have access to business systems and emails anymore. Establish a procedure for employees that are terminated, have a job status change, as well as new employees. These procedures should contain the necessary steps to permit or revoke access from resources depending on their job state.

8. Anti-virus software

Install and use this software on all computing devices.

9. Vendor Compliance

If you need to comply with regulations such as PCI, then process your credit card transactions using a vendor that complies with this regulation. Regularly obtain copies of compliance attestation letters from your third-party vendors that are responsible for storing, processing, or transmitting your sensitive information.

10. Email Security Gateway

Using this system will check incoming emails for viruses, malware, spam, and other types of attacks before the email arrives to your users' inbox.

11. Virtual Private Network (VPN)

This will ensure that, if anyone connects to your network, they will be unable to monitor or access the data you are sending over the network, for example, the password you are using to log in to different apps.

BONUS SECTION (PAID SERVICES)

ADVANCE SECURITY

IMPLEMENTING CYBER SECURITY ON A $10-15K ANNUAL BUDGET

1. User Awareness Training (free/cheap training content available)

Knowledge is the best firewall. Invest in user awareness training on a consistent basis. Organizations such as **Infosec Institute** can personalize security education solutions that are engineered to help you and your employees stay one step ahead of cyber threats.

2. Internal/External Penetration Test & Vulnerability Assessment

After you have the basics covered, you may want to hire a company that will attempt to hack your organization. This will give you an idea of how well you are protected against cyber attacks and what else can be done to better protect your business. **Vonahi Security's** automated network penetration testing platform, **vPenTest** includes a vulnerability assessment as an added value and at no extra cost to your organization.

3. IT Security Risk Assessment

An information security risk assessment can help your organization evaluate its entire information security program and allow your organization to develop processes to identify and mitigate security risks.

4. Security Information and Event Management (SIEM)

Almost all network systems (e.g. network devices, workstations, servers, etc.) have the capability to produce logs based on interactions from client-initiated activities, such as authentication attempts, shutdown/restart attempts, etc. These logs can be valuable for early detection of cyber attacks or investigating an ongoing attack. These logs can be very large in size and a centralized logging and monitoring solution is recommended to aggregate and analyze such logs.

5. Endpoint Detection & Response (EDR)

This software is the next generation of Anti-Virus and goes beyond scanning just traditional malware that resides on the hard drive. For example, EDR solutions have the capabilities of detecting malicious network activities originating to and from a host, as well as detecting advanced, sophisticated local attacks that attempt to bypass traditional anti-virus detection capabilities.

6. Web Content Filtering

Because visiting infected websites is often a main vector of attack for hackers, it makes sense to whitelist the websites your business uses for its operations. Whitelisting involves only allowing employees access to websites that have been added to the list of approved sites, all other sites are blocked.

7. Data Loss Protection (DLP)

Prevents sensitive information from leaving your business.

RESOURCE GUIDE

Free Security Resources

Internet Exposure Scout: https://www.vonahi.io/free-tools
Google's Free Phishing Quiz: https://phishingquiz.withgoogle.com
SSL Best Practices Website Checker: https://www.ssllabs.com

Authentication Resources

Securing Key Accounts & Devices: www.lockdownyourlogin.org
The Ultimate Guide to Two-Factor Authentication (2FA): www.turnon2FA.com
Two Factor Auth (2FA): www.twofactorauth.org

Stay up-to-date on the latest scams by signing up your employees for these alerts:

Federal Trade Commission Scam Alert: www.consumer.ftc.gov/scam-alerts
Better Business Bureau Scam Alert: www.bbb.org/council

Other Online Safety Resources:

Tips, posters and video for kids, home, business and mobile:
www.staysafeonline.org

FTC Cybersecurity for small businesses:
www.ftc.gov/smallbusiness

Bulk Order Free FTC Materials:
www.bulkorder.ftc.gov

NIST Small Business Cybersecurity Corner:
www.nist.gov/itl/smallbusinesscyber

NIST Cyber security is Everyone's Job Guidebook:
https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job

DHS Cyber security Resources Roadmap for Critical Infrastructure (SMB):
www.us-cert.gov/resources/smb

DOJ Cyber Incident Preparedness Checklist:
www.justice.gov/criminal-ccips/file/1096971/download

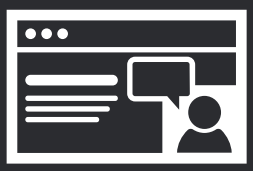
DFARS Cybersecurity Requirements:
https://business.defense.gov/Small-Business/Cyber security

Ransomware Keys:
www.nomoreransom.org

Report Cybercrime:
www.ic3.gov

ABOUT US

Vonahi Security is building the future of offensive cyber security consulting services through automation. We provide the world's first and only automated penetration test that replicates full attack simulations with zero configuration. With over 30 years of combined industry experience in both offensive and defensive security operations, our team of certified consultants have experience working with a significant number of organizations, industries, networks, and technologies. Our service expertise includes Managed Security, Adversary Simulations, Strategy & Review, and User Education & Awareness. Vonahi Security is headquartered in Atlanta, GA.



www.vonahi.io

Visit it our website to learn more about our services, schedule a demo, or request a quote.

HELLO WORLD.
MEET MODERN SECURITY.

VONAHI SECURITY

www.vonahi.io

info@vonahi.io

1.844.VONASEC (866-2732)

@vonahisec