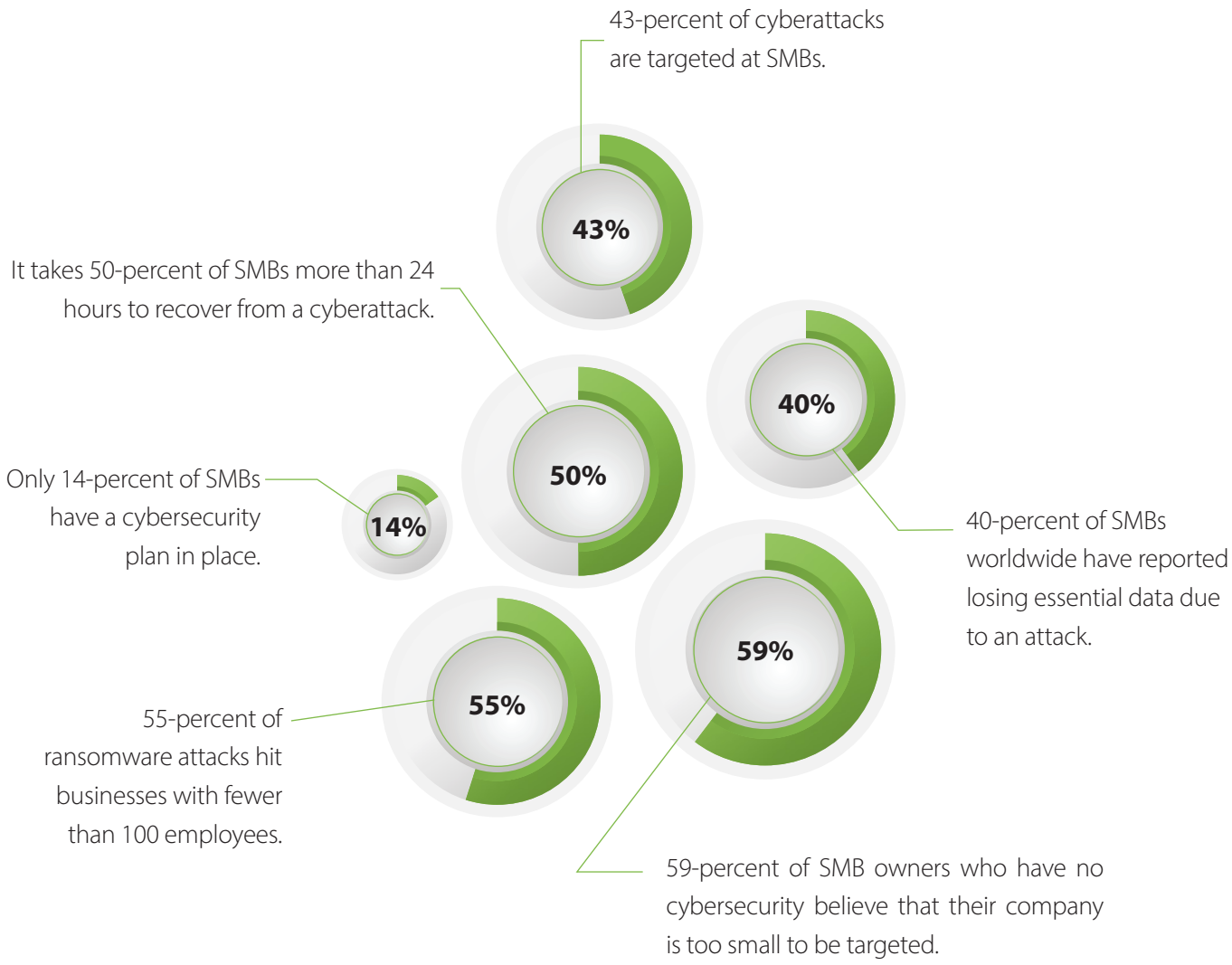
SECURANCE CONSULTING
the advantage of insight

Proactive vs Reactive Security: Network Hardening Strategies for SMBs

INTRODUCTION

Organizations of all sizes and in all industries are susceptible to ever-evolving ransomware attacks and cyber threats. Small- and medium-sized businesses (SMBs), in particular, face the brunt of many such attacks, and, unfortunately, suffer worse consequences, due to inadequate budgets, IT resources, and security awareness or knowledge. Avoiding and mitigating cyber threats requires organizations and individuals alike to steer away from a reactive approach, and instead take a proactive stance to cybersecurity. By "hardening" networks and systems (i.e., implementing security best practices, controls, techniques, and security tools), SMBs can minimize IT risks and reduce costs, loss of data, and recovery time when a cyberattack or data breach occurs.

2023 SMB Statistics



Astra, 2023[1]

WHAT IS NETWORK HARDENING?

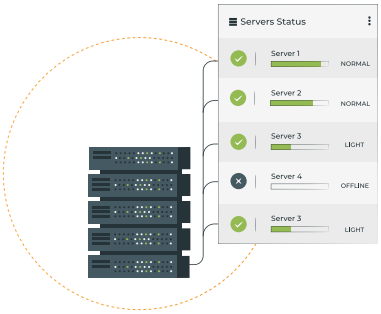
Network hardening means using tools, techniques, and best practices to reduce vulnerabilities in applications, systems, infrastructure, firmware, and other technologies. The goal of network hardening is to reduce security risk by eliminating potential attack vectors and minimizing the threat surface. By removing superfluous programs, account functions, applications, ports, and permissions, cybercriminals have fewer opportunities to gain access to the IT environment. There are multiple types of network hardening activities, including:

Application Hardening

Operating System Hardening

Server Hardening

Endpoint Hardening



Database Hardening

System Hardening

Network hardening is necessary throughout the technology life cycle, from installation and configuration, to maintenance and support, to decommissioning. Network hardening is also required by regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA) and, increasingly, by cyber insurers.[2]

> Most SMBs do not invest in the level of IT security they need. As a result, a ransomware attack or data breach leaves them with millions of dollars in remediation costs. Many SMBs go under after a single cyberattack. This is why network hardening is so important.[3]

KEY BENEFITS OF NETWORK HARDENING

The most notable benefits of network hardening include:

- **Better security**— When done correctly, network hardening can significantly reduce the chances of a successful cyberattack. By minimizing the threat surface, network hardening lowers the risk that your environment will be compromised.
- **Improved performance**— Part of network hardening includes removing unnecessary technologies, applications, permissions, and systems. By doing so, bad actors have fewer entry points and staff have improved management and greater visibility within the IT environment. Working with limited, but vital, hardened systems and programs means you can monitor them better and ensure they function optimally.
- **Cost savings**— Secure networks and systems mean fewer cyber incidents and less money spent on recovery efforts. Hardening also saves maintenance costs by removing unnecessary hardware and software.
- **Simplified audits**— Fewer applications and programs translates a less complex infrastructure, making auditing more straightforward and manageable.[4]

COMMON NETWORK SECURITY THREATS

Malware

Malware is malicious software that can spread across computer systems, and can be used to compromise a device or damage data and systems. The most common form of malware, ransomware, encrypts data, making it inaccessible to users until an encryption key is provided. Its primary distribution vectors are email, malicious links, and compromised websites.

Distributed Denial of Service Attacks

A distributed denial of service (DDoS) attack leverages a botnet to flood networks with fake traffic, ultimately causing the targeted network or system to crash. Sometimes, the goal of a DDoS attack is to distract IT and security teams while the hackers launch a bigger attack. The most effective defense is a third-party DDoS mitigation solution.

Insider Threats

Insider threats can include disgruntled employees, compromised accounts, negligent insiders who violate security policies, and unaware users who delete data by accident. Insider threats are difficult to detect with traditional security tools, and because insiders have privileged access to sensitive systems, they can be very dangerous.[5] Fostering a culture of security awareness is the best tool any organization can adopt to mitigate insider threats and human error.

> Network security requires multiple layers of defense from the network edge to the core. That includes ensuring identities, devices, applications, data, and systems are protected from unauthorized access at every point. Network security strategies must stop the bad guys from entering the network and prevent them from traveling once they are inside.[6]

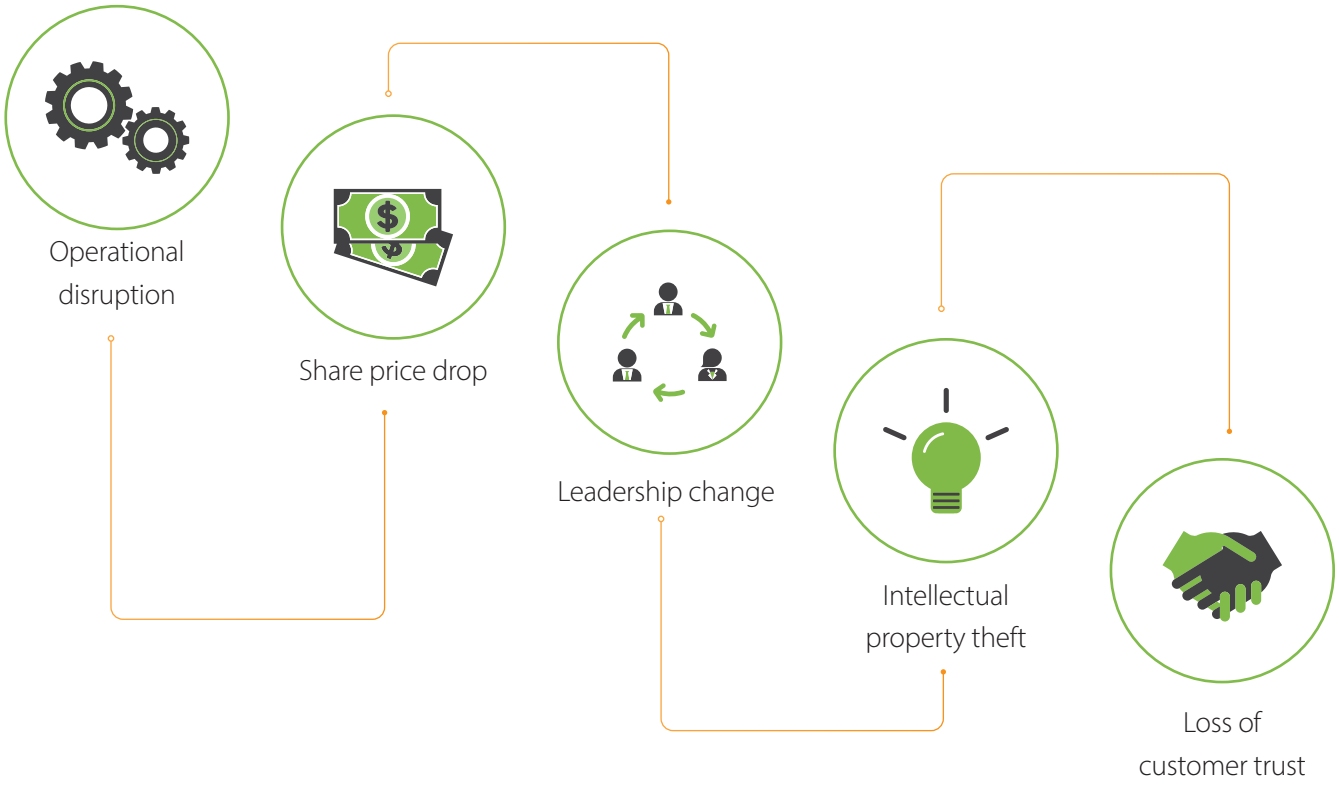
Man-in-the-Middle Attacks

Man in the middle (MITM) attacks occur when a bad actor listens in on a private communication. This can include IP spoofing, Wi-Fi hacking, and intercepting emails, text messages, phone calls, or any other communication between two parties. Cybercriminals can use their access to spoof messages, delete or alter data, or engage in social engineering attempts.[7]

Cloud Security

As organizations continue to gravitate toward the cloud for data storage, retrieval, and accessibility, bad actors have also found ways to infiltrate it. Without proper cloud security tools, management, and policies and procedures in place, organizations can introduce additional vulnerabilities to their environments.

Common Consequences After a Cyber Incident



NETWORK HARDENING STRATEGIES

Network hardening varies between computing systems, and there may be different hardening procedures for unique components of the same system. However, there are general hardening tasks applicable to most computing platforms. Consider these eight critical tasks to harden your networks and systems.

Govern Access

Organizations should enforce the principle of least privilege and role-based access control (RBAC) to reduce the number of permissions and users that have access to the networks. This is one of the most effective security practices to reduce the overall attack surface.

Update, Update, Update

Applications, browsers, and operating systems should be monitored and updated regularly, so that your organization is running the most current versions. Security patches should be applied as soon as they become available.

Traffic Control

This step can include:

- Configuring the firewall to allow only specific traffic to known services.
- Requiring a virtual private network (VPN) for remote access.
- Disabling unnecessary privileges for remote sessions.
- Monitoring logs for unusual logins and activity.

Polish the Threat Surface

Unnecessary software, services, and features should be disabled or uninstalled if not in use. Any component or application feature that is operational, but not in use, expands the threat surface.

Ongoing Management

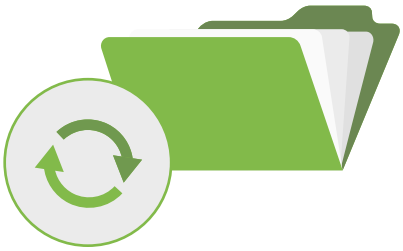
Organizations should regularly review logs for anomalous activity, with a special focus on authentication, user access, and privilege escalation. Mirror logs to a separate location to protect log integrity and avoid tampering. Perform regular vulnerability and malware scans, and if possible, conduct an external audit or penetration test at least once a year.

Secure Communications

Encrypt data transfer using strong ciphers. Close all but essential network ports, and disable insecure protocols, like SMBv1, Telnet, and HTTP.

Regular Backups

Hardened systems are sensitive resources and must be regularly backed up using the 3-2-1 rule (three copies of the backup, on two types of media, with one copy stored off-site).



Harden Remote Sessions

If the organization uses Secure Shell (SSH) network protocols to access and communicate with remote machines, ensure a secure password or certificate is used. Additionally, your organization should disable elevated privileges for SSH access, monitor SSH logs to identify anomalous use or privilege escalation, and avoid using default ports.[8]

> With new technology and threats emerging almost daily, SMBs must use every tool in the box to minimize the potential for cyberattacks. The hardening process eliminates unneeded programs, accounts, and access that increase the likelihood of compromise and data loss.[9]

CONCLUSION

Hardened Networks, Systems, and Mindsets

Default configurations of technologies may be convenient, but they are almost never optimally secure. Without hardening, these technologies are vulnerable to malicious attacks and at high risk for compromise. By performing regular updates, governing access, securing communications, and implementing the proper tools, techniques, policies, and security controls, SMB owners can protect their company, employees, customers, and reputation, minimize the threat surface, and streamline recovery efforts when an incident or breach does occur.

For organizations that need help getting started, Securance offers the first-ever Online Hardened Network Security Assessment. This free tool provides an immediate, customized report with your organization's security maturity rating intended to help build a secure, reliable IT environment.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/
2. https://www.beyondtrust.com/resources/glossary/systems-hardening
3. https://www.tworivercomputer.com/hardening-your-network/
4. https://www.enterprisenetworkingplanet.com/security/system-hardening
5. https://www.catonetworks.com/network-security/network-security-threats/
6. https://delinea.com/blog/network-security-and-hardening
7. https://www.cimcor.com/blog/top-5-network-security-risks-and-threats
8. https://perception-point.io/blog/system-hardening-guidelines-for-2022-critical-best-practices/
9. https://www.odi-x.com/news/blog/what-is-the-value-of-cis-hardening/

Proactive vs Reactive Security: Network Hardening Strategies for SMBs

SECURANCE CONSULTING
the advantage of insight

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com