Protect Business Growth with Cybersecurity

Networks have grown more complex. Businesses are moving their services to multiple cloud vendors, and even though cloud services are generally secure, nothing is perfect. With nearly any cyberattack—and especially with cloud services—email remains a key method cybercriminals use in a breach. Protecting email must be an essential part of a larger security strategy.

Business Growth Depends on Secure Environments

90% of c-level executives feel public trust in the security of the internet is essential for businesses growth.[1]

As dependency on the internet grows, so do security risks. You are at risk even if you think:

- You don't have a lot of assets, or valuable information anyone wants
- You don't have a large amount of money to steal
- You aren't a big enough company to be a prime target

Keeping businesses secure online builds a foundation for growth by:

- Boosting uptime
- Increasing productivity
- Reducing time and resources spent mitigating cyberthreats and dealing with breaches
- Demonstrating compliance
- Protecting intellectual property and business data
- Maintaining good business and brand reputation
- Reducing customer churn

Your Customers Are Prime Targets

67% of SMBs have faced a cyberattack, and **58%** experienced a data breach.[2]

The consequences can be dire: The average time to detect and contain a breach is estimated at **279 days**.[3]

40% of companies are down more than 8 hours after a breach.[4]

A Strong Security Foundation Can Help Reduce Your Customers' Risks

Secure Your Own MSP

- Practice the fundamentals by patching, putting up firewalls, running backup, and employing professional email security in house
- Understand what applications are in use, and who should have access.
- Invest in advanced endpoint protection solutions for your own machines.
- Monitor for threats to your network with security information and event management (SIEM) tools.
- Use a password management tool to maintain strong password security.

Mitigate Risk with Layered Security

- Assess your customers' risks.
- Implement the right layers to mitigate risks including:
  - Mail protection
  - Web protection
  - Patch management
  - Network protection
  - Identity management
  - Firewall management
  - Managed antivirus
  - Threat monitoring
  - Endpoint detection and response
  - Backup
  - Vulnerability scanning
  - Password management
  - Disk encryption

Educate Your Customers

- Establish and maintain a culture of security for your customers with regular training and awareness.
- If needed, team up with third parties to help with security awareness training.
- Teach users to spot malicious emails or other social engineering attempts, with examples.
- Retrain users on an on-going basis—security training should be regular and frequent to get the results you need.

Email Protection Should Be Part of Your Security Strategy

Cybercriminals **love** email:

53% of email traffic is spam[6]

93% of breaches are a result of phishing attacks and pretexting[7]

84% of social attacks involved phishing emails[8]

53% of midmarket organizations have been victim to a breach[9]

Email was the most common point of entry for malware in 2018 – 2019[5]

One malicious email can cause a lot of damage and halt growth. Make sure to employ professional-grade email protection to help prevent malware from getting into your—and your customers'—networks.

Help Prevent Email Threats from Stopping Growth with N-able Mail Assure

N-able™ Mail Assure provides cloud-based email security to help your customers stay in control and protect their inbound and outbound email using collective intelligence.

Start free trial

1"Securing the Digital Economy: Reinventing the Internet for Trust," Accenture. accenture.com/_acnmedia/Thought-Leadership-Assets/PDF/Accenture-Securing-the-Digital-Economy-Reinventing-the-Internet-for-Trust.pdf#zoom=50 (Accessed January 2020).
2"2018 State of Cybersecurity in Small & Medium Size Businesses," Ponemon Institute. keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf (Accessed January 2020).
3"Cost of a Data Breach Report, 2019," IBM. databreachcalculator.mybluemix.net/ (accessed January 2020).
4"Cisco 2018 Cybersecurity Report: Special Edition SMB," Cisco. cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf (Accessed January 2020).
5"2019 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf (Accessed January 2020).
6"'Abuse Emails': What They Are and How They Impact Your Email Marketing," Entrepreneur. https://www.entrepreneur.com/article/335272 (Accessed January 2020).
7"2018 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/dbir/ (Accessed January 2019).
8"2019 Data Breach Investigations Report," Verizon. enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report-emea.pdf (Accessed January 2020).
9"Cisco 2018 Cybersecurity Report: Special Edition SMB," Cisco. cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf (Accessed January 2020).

About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com