

Why SMBs, Not Just Large Businesses, Are Targets for Cyber Attacks



66% of small and medium business leaders don't believe they are vulnerable to cyberattacks.

Headlining the news lately has been a string of high-profile cyber attacks. Since December 2020 and the Sunburst attack on SolarWinds Orion platform, there has been a steady stream of significant incidents, including several ransomware attacks. Fueled by the anonymity afforded by payments made in cryptocurrency, cybercriminals stepped up their attacks on entities such as critical infrastructure (Colonial Pipeline) and food production (JBS Foods). Not only have attackers gotten bolder with their targets, the ransoms demanded have also increased and are often millions of dollars. In fact, because they are receiving such large amounts, cybercriminals continue to be motivated to carry out new attacks. They have also figured out that by carrying out attacks that disrupt society, such as the gas and meat shortages caused by the attacks on Colonial Pipeline and JBS Foods, that they are more likely to have their ransom demands met more quickly.

2022 High Profile Cyberattacks

- Nelnet Student loan provider data breach of 2.5 million student social security numbers¹
- Optus data breach 11 million medical and personal records in Australia²
- What'sApp data from almost 500 million users went up for sales on the dark web³
- Microsoft, Uber and News Corp (publisher of the Wall Street Journal) also experienced cyberattacks in 2022

While these attacks where large companies pay million dollar ransoms become headline news, what is often overlooked in the media attention is that cyberattacks actually happen more often than reported. Most attacks aren't newsworthy, and they don't always target large businesses. In fact, malicious actors target businesses of all sizes, including small and medium businesses (SMBs). According to the [Verizon's 2022 Data Breach Investigations Report](#), (DBIR), 46% of cyber attacks target small businesses.

Why SMBs are Targets of Cybercriminals

While IT security is viewed as a priority for most businesses, small businesses are particularly vulnerable to cyberattacks. To begin, the fact that they are a smaller business means they don't have the same IT staff in place as large companies, or the large budgets required to shield them from the ever-increasing number of attacks. Simply not having the resources available, and therefore less robust security, puts SMBs at a disadvantage to prevent and mitigate a cyberattack.

51% of small businesses do not have protection against cyberattacks⁴

SMBs are also often quick to downplay the risks of cyberattacks and adopt the "it can't happen to me" mentality. According to a [survey](#), 66% of small and medium business leaders don't believe they are vulnerable to cyberattacks. This tendency to downplay threats happens even as SMBs increase their attack surfaces with the addition of remote and hybrid workers, using more apps and online systems, and adding more and more IoT devices to the network. This attitude also leads to lax security practices among them being weak passwords, ineffective mobile device policies, and not keeping up with cybersecurity threats.

59% of small business owners who don't have cybersecurity measures in place say their business is 'too small' to be a target⁵

There is also a tendency amongst SMBs to assume their data isn't as valuable as data of larger companies. However, that is not the case. Healthcare practices, small retail, nonprofits and other small to medium businesses all have information that hackers will find valuable to hold for ransom or sell on the dark web. Credit card numbers, medical records, financial information, social security numbers, product information and confidential business information collected by SMBs are all valuable to cybercriminals. These are often easily more accessible to bad actors than large enterprises due to less robust security.



Even more nefarious than stealing critical data and information, malicious actors also use hacking smaller companies to infiltrate more companies and/or larger entities. While larger companies may have more robust cybersecurity measures in place that are harder to penetrate, SMBs can be the gateway to enter larger organizations. Today's businesses are digitally connected with many SMBs having access to the systems of larger organizations to conduct business such as transactions, share information and manage supply chains. Hackers see these connections as a way to access the systems of larger entities.

Perhaps the most well-known attack of this sort is the infamous 2013 data breach of Target where hackers stole data from up to 40 million credit and debit card holders. It was later reported that the initial intrusion into its systems was traced back to network credentials that were stolen from a small, third-party HVAC vendor.

The [Kaseya VSA](#) ransomware attack targeted the tool that MSP's trust to manage and gain access to all their clients' systems, giving the cybercriminals a way to infiltrate more businesses than if they were to go after them one at a time. While Kaseya said that only approximately 50 of its customers that use the on-premises VSA had been directly compromised, it's estimated that 800 to 1500 SMBs had been infiltrated and affected by the attack.

Top Cyber Threats to SMBs

SMBs face the same attack methods as larger businesses, yet often with fewer resources and are often less prepared to fight them. To protect against cyberattacks, SMBs must understand the threats they face and how hacks can occur.

Malware / Ransomware

Malicious attacks by malware software are designed to cause harm with some of the most common being Trojans, viruses, spyware, adware and bots. While all behave differently, they can spread throughout a system undetected, especially by small businesses. The purpose of malware is to make money such as by accessing accounts or credentials, blackmailing victims with stolen sensitive data or stealing industry secrets. The impact of a malware attack can be detrimental to the company's network, data and reputation.

Ransomware has become the most popular, high-profile, and devastating form of malware and is affecting both large and small businesses at an alarming rate. This form of malware infects a network and denies access unless a ransom is paid. Refusing to pay the ransom could result in a loss of data, however, paying does not guarantee a restoration of the data or immunity from future attacks.

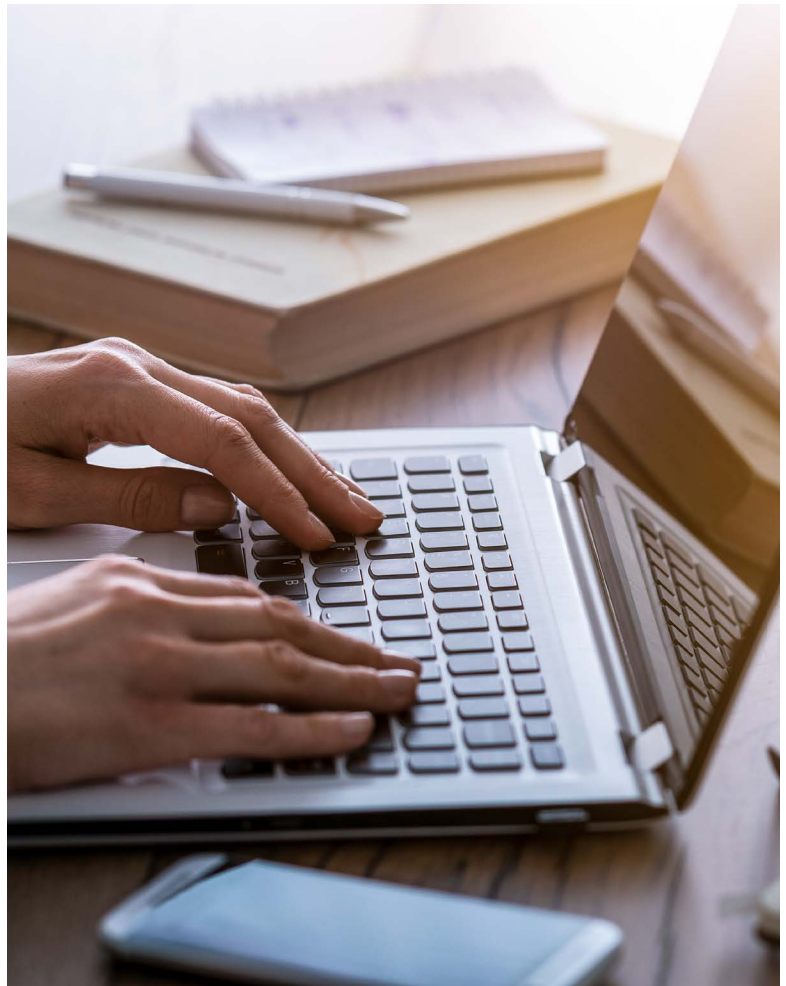
Phishing and Social Engineering

To deploy malware, criminals use tactics such as phishing and social engineering to entice people to unsuspectingly download malicious software and give them a path to enter the network.

Phishing emails appear to be similar to other emails reaching your inbox but have clearly identifiable signs that they could be spam and malicious. While it may look like it is from a trusted source, there are tell-tale signs it is a hacker:

- Incorrect domain name in email address
- Urgent or threatening language
- Suspicious attachments or incorrect links
- Misspelled words or grammatical errors
- Mismatched URLs

Social engineering emails get more specific and polished in their targeting and appear to be a personal email. For example, they send an email that looks like it's from a CEO to employees, however, it's a fraudulent email usually with a malicious link or document to download.



Human Factor

A favorite statistic of cybersecurity pundits is that 95% of cybersecurity breaches are due to human error. Cybercriminals aim their attacks at careless employees who trustingly click on unknown links, fail to regularly change their passwords, download unauthorized Internet applications onto their computers or don't update their software.

Insider threats are also a hazard for SMBs. Unfortunately, there are employees, current or former, who have bad intent against the company and can unleash an attack. Insider threats aren't limited to employees, they can also be a vendor, contractor or associate who has access to critical information. Proper off-boarding of employees as well as network segmentation, access to only the information needed to do the job, should be standard practices to address potential insider threats.

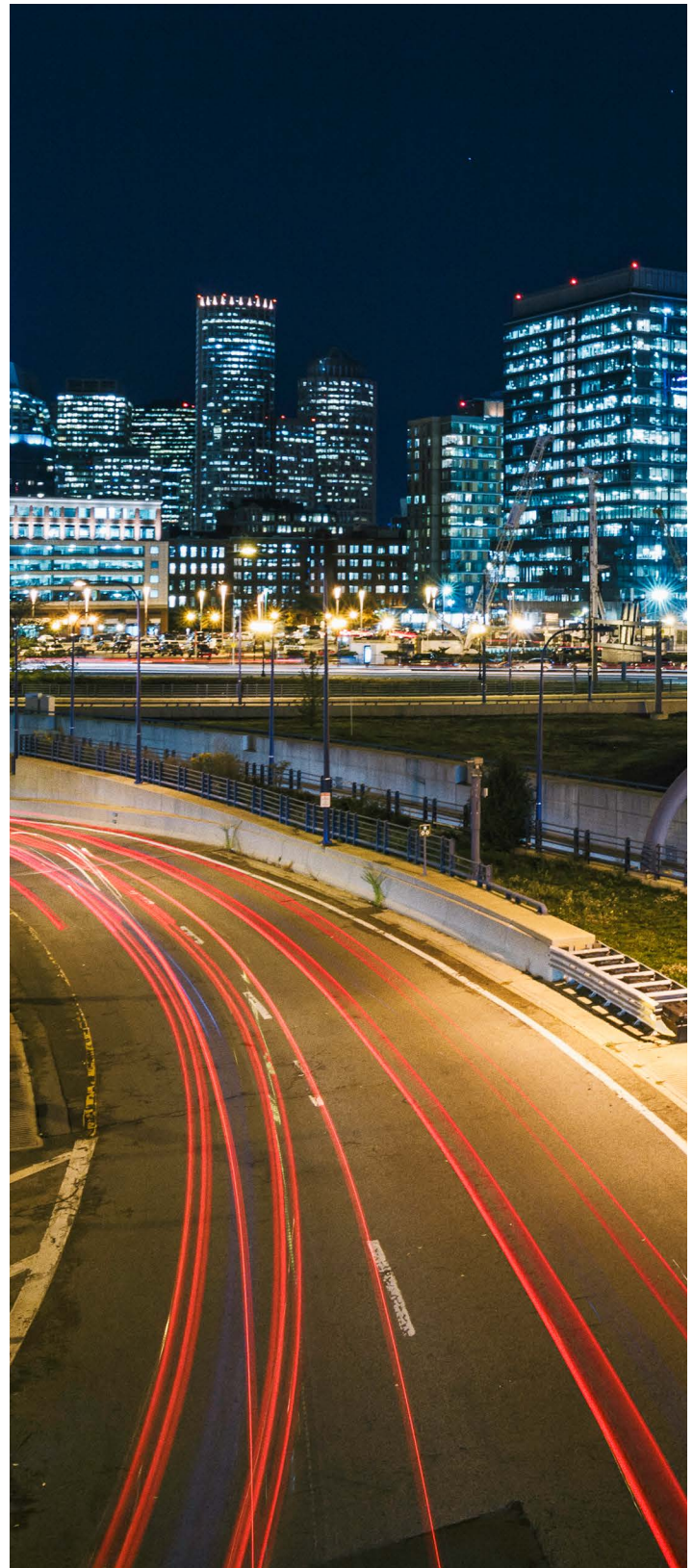
Spotting a Hack

While large corporations have the resources in place to detect a breach, smaller companies with fewer detection and security measures in place, rely on themselves and employees. Being able to recognize suspicious activity can help SMBs spot the attack and minimize damage. Businesses should look for the following to identify an attack:

- Unusual activity
- Changes in user access
- Suspicious file changes
- Battery draining quickly
- Unknown devices on your Wi-Fi
- Unexpected network behavior

Consequences of Attack

While SMBs may feel invincible against a cyberattack, the consequences of being a victim can be devastating. After an attack, businesses not only have to recover data, but they must also invest in fixing the damaged portions of their network. In addition, they must now also be concerned with possible lawsuits and reputational damage and loss of trust to their business. Because of these factors, 60% of companies go out of business within six months after a data breach.⁶



One example is [Wood Ranch Medical](#), a clinic that was located in Simi Valley, CA. They were the victims of a ransomware attack that was so malicious that their computer systems were permanently damaged and even the backups were encrypted. Unable to recover the records of almost 6,000 patients, they were forced to close within months.

What SMBs Can Do to Protect Their Business

First and foremost, to protect small and medium businesses from cybercriminals, company leaders need to take the threat of an attack seriously and understand the consequences. With limited budgets, SMBs may not be able to employ an MSP, but there are measures every company can take to protect themselves:

- Conduct a cybersecurity risk assessment audit to determine data risks and the appropriate preventive measures that must be taken.
- Train employees continuously. As security adversaries find new ways to infiltrate networks, keeping employees trained and up to date will only strengthen your network security.
- Use multi-factor authentication to provide an additional layer of protection of sensitive data.
- Backup your data. If your data is backed up, even if your network is breached, a backup can revert the machine to the data it had on it the day before the attack, minimizing losses.
- Segregate your network to isolate and minimize a ransomware attack. Set up separate networks for different types of usage and/or roles. For example, have a guest network that is completely separate to the main network.
- Keep software updated: update and install all software patches expediently to avoid a breach.
- Develop an incident response plan in the event that you experience a breach. This will outline steps to take to mitigate the attack and recover.

Sources

1. <https://www.cshub.com/attacks/news/student-loan-data-breach-leaks-25-million-social-security-numbers>
2. <https://www.cshub.com/attacks/news/iotw-everything-we-know-about-the-optus-data-breach>
3. <https://www.cshub.com/attacks/news/hacker-attempts-to-sell-data-of-500m-whatsapp-users-on-dark-web>
4. https://www.prweb.com/releases/digital_com_survey_reveals_more_than_half_of_small_businesses_do_not_have_cybersecurity_measures_in_place/prweb18578953.htm
5. <https://digital.com/51-of-small-business-admit-to-leaving-customer-data-unsecure/>
6. <https://www.forbes.com/sites/emilsayegh/2022/08/16/businesses-shutting-down-business/?sh=7e2b86514cc6>

Other Resources

- [166 Cybersecurity Statistics and Trends for 2022](#)
- [Verizon 2022 Data Breach Investigations Report](#)
- [Ransomware Payouts in Review. Highest Payments, Trends & Stats](#)
- [Brenntag sheds light on DarkSide ransomware attack](#)
- [The State of Small Business Cybersecurity in 2021](#)
- [8 Reasons SMBs are a Top Target for Cyberattacks](#)
- [Target Hackers Broke in Via HVAC Company](#)
- [The Disturbing Facts About Small Businesses That Get Hacked](#)
- [Hackers Are Targeting Your Small Business](#)



About Arista's Cognitive Unified Edge (CUE)

Arista's CUE solutions help SMBs and distributed enterprises optimize their networks while safeguarding their data and devices. CUE redefines networks with enhanced security and connectivity, flexible PoE switching, and Wi-Fi 6/6E offerings that work together seamlessly to ensure connectivity, protection, monitoring, and control across the entire network from headquarters to the network edge.

Centralized Cloud Based Management

- Visibility across globally dispersed networks & endpoints
- Zero touch deployment for hardware appliances
- Advanced alerting & reporting for CIPA compliance

Next Generation Firewall

- Next-gen firewall, with IPS, VPN & more
- Protection, encryption, control & visibility anywhere
- Onboard security for small network appliances & IoT devices
- Full security processing on-premises or in the cloud

WAN Optimization

- Secure, WAN-optimized connectivity for every location
- Seamless scalability with centralized policy management
- Optimal predictive routing technology for first packet, dynamic path selection

Wired Connectivity

- Scalable PoE compact switches with 12 to 48 ports
- Based on Arista's Extensible Operating System (EOS)
- Wire rate encryption/tunneling
- Multi-gigabit uplink speeds from 1 to 100 Gbps

Wi-Fi 6 Access Points

- Enterprise class Wi-Fi 6 and Wi-Fi 6E technologies
- Optimized performance to scale from 1 to hundreds of users per AP
- Multi-gigabit uplink choices based upon bandwidth needs
- Open, published APIs for integration with ITSM and monitoring tools

Santa Clara—Corporate Headquarters

5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500

Fax: +1-408-538-8920

Email: info@arista.com

Ireland—International Headquarters

3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office

9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office

Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office

9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989



Copyright © 2023 Arista Networks, Inc. All rights reserved. All other company names are trademarks of their respective holders. Information in this document is subject to change without notice. Certain features may not yet be available. Arista Networks, Inc. assumes no responsibility for any errors that may appear in this document. March 6, 2023