CROWDSTRIKE

CrowdStrike Products

Solution Brief

Importance of Cybersecurity for Small Businesses

Securing your growing business and maintaining customer trust with modern cyber protection

Small business owners are wearing more hats than ever before. Along with managing operations, sales, engineering, innovation, customer satisfaction and more — on top of hiring and managing experts to lead those disciplines — owners must also stay on top of the latest trends that can impact their business trajectory, both positively and negatively. With cyber threats against small businesses on the rise, owners need modern, reliable cyber protection that is not only easy to use, but also trusted and affordable, to keep their business data — and their customers' data — safe.

Why Cybersecurity Matters for Small Businesses

As of 2023, 99.9% of all businesses in the United States qualify as small businesses — a total of 33.2 million.[1] Along with this vast number of small businesses comes a rise in job creation, technology usage, and business and customer data. At the same time, small businesses have witnessed a significant rise in cyber threats.

The CrowdStrike 2024 Global Threat Report identified year-over-year increases in tracked adversaries, cloud intrusions, data theft extortion and eCrime victims across the threat landscape, with many cyberattacks happening on small businesses.[2] In fact, **small businesses are 3x more likely to be targeted by cybercriminals than a larger enterprise.**[3]

But why are small businesses becoming the target of attacks? Adversaries have identified that in many cases, small businesses often lack the resources to fully shield themselves from such attacks. Adversaries are exploiting the vulnerabilities of growing businesses in order to gain access to vast amounts of data that can be sold for financial gain, identity theft, extortion or industrial espionage.

Important Terms

- **Cybersecurity:** The practice of protecting digital assets, such as networks, systems, computers and data from cyberattacks
- **Adversary:** A person or group that intends to perform malicious actions against other cyber resources; a cybercriminal
- **Ransomware:** A type of malware that encrypts a victim's data and then the attacker demands a "ransom," or payment, in order to restore access to files and network
- **Phishing:** A scam that impersonates a reputable person or organization with the intent to steal credentials or sensitive information
- **Malware:** An umbrella term that describes a program or code created to harm a computer, network or server, designed to infiltrate a system to steal or destroy data

[1] U.S. Chamber of Commerce Small Business Data Center

[2] CrowdStrike 2024 Global Threat Report

[3] Forbes, "Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report," March 16, 2022

But understanding the intricacies of cybersecurity and navigating its complex landscape can be particularly challenging. Along with identifying the right technology to protect data now, business owners need to think about future cyberattacks and ensure their solutions keep them safe. Investing in cybersecurity solutions now creates provable ROI, as the average cost of a data breach on small businesses is $3.31 million USD in 2023.[4] It also protects their business reputation from damage that could stem from a data breach. Small businesses also need to provide accurate and current training for employees on common cyber threats and the impact of data breaches, implement secure remote work policies, limit access to sensitive information and keep all security software up-to-date.

Small business owners need to recognize that, without those effective and proactive cyber protections in place, they run the risk of shutting their doors altogether. In a recent TechValidate survey, 35% of small business owners stated that they would “likely” or “definitely” go out of business in the event of a cyberattack.[5] Reductions in operational efficiency, loss of intellectual property and the theft of customer data all pose significant risk to the success of a small business, and the confidence instilled in them by their customer base. Customer trust is the most valuable asset for any small business, and something that must be protected in order to secure the business’s future.

By the Numbers

- 99.9% of all U.S. businesses qualify as small businesses
- 60% of small businesses say cyber threats (phishing, malware, ransomware) are a top concern[7]
- 35% of small business customers would “likely” or “definitely” go out of business if they suffered a cyber breach
- 33% of small business customers are concerned about customer data theft[8]
- 30% of small business customers are concerned about loss of business productivity in the event of a cyberattack[8]

Importance of Customer Trust

In an era where cyber threats are ever-present, securing customer data is not just a priority but a necessity. Customer data is a highly valuable asset, making it a prime target in any attack. The CrowdStrike 2024 Global Threat Report identified a 20% increase in access broker advertisements on the dark web selling customer data that can be used for identity theft, for making fraudulent purchases or for phishing attempts to gain access to even more data.

Small business owners are aware of the value of their customers’ data. The TechValidate survey found that 33% of small business owners listed customer data theft as a top concern that could affect their business.[6] If there is a data breach and customer data is compromised, trust is lost and the customer can take their business elsewhere.

Small business owners recognize that their business will only succeed if they can both earn trust from new customers and keep that trust to retain customers. With modern cybersecurity protections, small business owners can alleviate their concerns about customer data theft.

Benefits of a Modern Cybersecurity Solution

A reliable and effective cybersecurity solution can give small business owners peace of mind that their business and customer data is secure.

- **Protection for sensitive business information:** Cybersecurity measures help safeguard confidential business and customer data from breaches and theft, thereby maintaining trust.
- **Regulatory compliance:** Reaching and maintaining compliance with data protection regulations helps meet the requirements of governing bodies across key industries.

[4] IBM Cost of a Data Breach Report 2023
[5] TechValidate survey of CrowdStrike Small Business Customers, April 2024, n=143
[6] TechValidate survey of CrowdStrike Small Business Customers, April 2024, n=143
[7] U.S. Chamber of Commerce Small Business Data Center
[8] TechValidate survey of CrowdStrike Small Business Customers, April 2024, n=143

- **Minimized financial loss:** By preventing cyberattacks, small businesses can avoid the significant financial costs associated with data breaches, ransomware and other cyber threats, which would otherwise lead to loss of revenue and hefty recovery expenses.
- **Improved business reputation:** A strong cybersecurity posture enhances a company's reputation by demonstrating commitment to protecting customer data, which can attract more customers and business partners.
- **Operational continuity:** Effective cybersecurity helps ensure that business operations are not disrupted by cyber incidents, maintaining productivity and service delivery.
- **Competitive advantage:** Small businesses that prioritize cybersecurity can differentiate themselves from competitors by offering secure services and gaining the trust of clients who are increasingly concerned about data security.

CrowdStrike Solutions for Small Businesses

Small business owners can take advantage of the same enterprise-quality cybersecurity, protecting their business information and customer data from outside attacks that would be detrimental to their business.

Learn how CrowdStrike's secure, easy-to-use and affordable cybersecurity solutions can protect your small business from attacks.
https://www.crowdstrike.com/solutions/small-business/

What CrowdStrike Small Business Customers Are Saying

"Perfect solution for a small company. In less than an hour, everything was running perfectly."

"CrowdStrike gives our small company the peace of mind that we have eyes on our system at all times."

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.