White Paper

halcyon

Ransomware Attacks: The Risk & Impact to SMBs

Small and Medium Businesses Under Siege

Attacks against SMBs (small and medium-sized businesses) have surged at an alarming rate based on findings from the 2025 Verizon Data Breach Investigations Report (PDF).

Malicious actors frequently target these organizations by taking advantage of their constraints and limited infrastructure and as security incidents and ransomware multiply across industries, SMBs now stand directly in harm's way while working hard to safeguard their core business functions and data.

Key Findings from the 2025 Verizon DBIR Report:

- Ransomware is the most significant threat to SMBs, accounting for 88% of SMB breaches.
- Threat actors are increasingly targeting SMBs due to their limited security resources and infrastructure.
- SMBs are often used as entry points for supply chain attacks, impacting larger organizations.
- Social engineering, malware (especially ransomware), and credential theft are the primary attack methods against SMBs.
- SMBs face significant financial and operational impacts from breaches, including downtime, loss of trust, and reputational damage.
- SMBs struggle with resource constraints, such as limited budgets and expertise, making them particularly vulnerable.
- Errors account for only 1% of SMB breaches, but malware and social engineering attacks are highly prevalent.

Threat actors are increasingly targeting SMBs due to their limited security resources and infrastructure.

halcyon

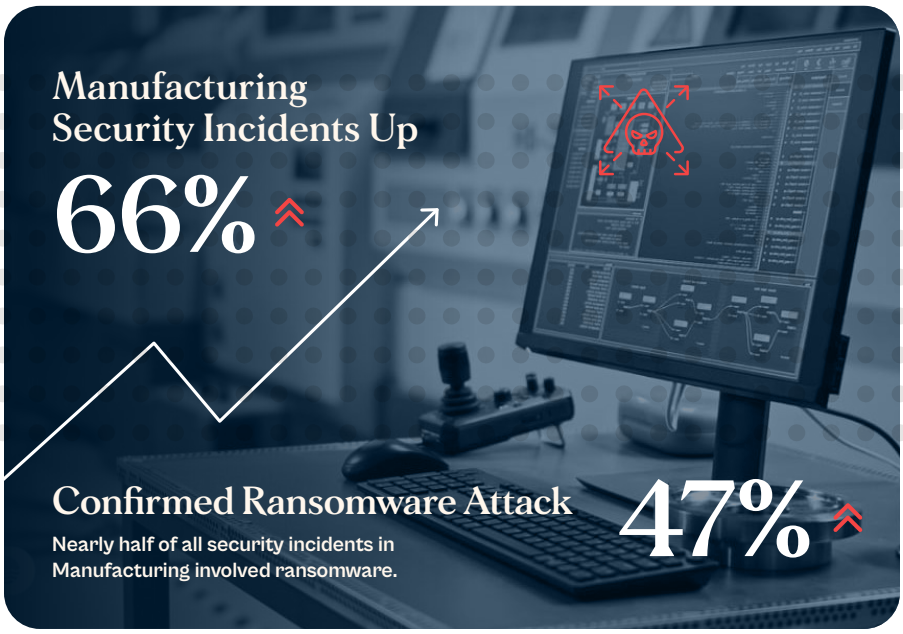
Ransomware as The Dominant Threat to SMBs

The data from the DBIR makes it clear that ransomware stands as the gravest risk SMBs face today. A stunning 88% of breaches in these organizations involved ransomware attacks, far surpassing the 39% rate seen in larger enterprises. To maximize their profits, threat actors have deliberately turned their attention to smaller businesses, taking advantage of their security gaps while monetizing their valuable digital assets.

Small businesses now face sophisticated attackers who have refined their extortion methods. Rather than selling stolen data on underground markets, these criminals force companies to make immediate payments to regain system access. Without proper recovery options, many small businesses see paying the ransom as their only way to resume operations.

Operators carefully adjust their financial demands when targeting SMBs. While large enterprises face million-dollar ransoms, operators target SMBs with lower amounts they can manage to pay. Subsequently, many small businesses view these reduced ransoms as an unavoidable cost when comparing them to extended business disruption and damaged reputation.

Threat groups now exfiltrate sensitive data before encrypting systems. By threatening both data exposure and system lockdown, they create immense pressure on SMBs to comply with their demands. Small businesses must prepare for two distinct challenges when faced with these attacks: managing encrypted systems and operational disruptions and developing strategies to handle potential data leaks. This dual threat means small businesses spend significantly more time addressing ransomware incidents, as they must handle both technical recovery and potential fallout from data exposure.



88%

Ransomware Targeted SMBs Dominantly

compared to

39%

of attacks on large enterprises involved ransomware.

21

Days of Downtime

Average days of operational downtime following a successful ransomware attack.

Key Tactics Used on Manufacturing:

34%

USE OF STOLEN CREDENTIALS

23%

VULNERABILITY EXPLOITATION

19%

PHISHING ATTACKS

halcyon

The impact is severe as ransomware incidents often lead to significant operational halts that prevent employees from accessing critical systems and data. The average downtime following a ransomware attack is around 21 days, severely disrupting operations and resulting in millions in lost revenue.

Evolution of Attack Strategies

Threat actors have evolved significantly in their approach to SMB targets, exploiting vulnerabilities specific to smaller organizations through scalable attack methods. By targeting multiple SMBs simultaneously, attackers maximize their returns while conserving resources.

Advanced persistent tactics have become increasingly common in attacks against SMBs, despite their traditional association with nation-state actors. Ransomware operators now spend extended periods inside compromised networks while gathering intelligence about their victims. They carefully time their ransomware deployments for optimal impact after thorough reconnaissance of organizational patterns.

Attack Vectors and Patterns in SMB Breaches

The DBIR reveals three primary attack methods targeting SMBs: system intrusion, social engineering, and basic web application attacks, collectively accounting for 96% of breaches. These attacks exploit both technical vulnerabilities and human error to gain unauthorized access.

Credential theft is a significant concern, with 33% of SMB breaches involving stolen credentials. Due to limited resources, smaller businesses struggle to detect and address these incidents, allowing attackers to maintain long-term access and gradually escalate their attacks.

Malware poses a particular threat to SMBs, with ransomware leading to nearly half of all malware-related incidents. Many organizations have suffered devastating operational impacts from these attacks. The manufacturing sector has seen malware incidents rise to 66% this year, up from 40-50% in previous years, with ransomware accounting for 47% of cases. Additional attack vectors in manufacturing include stolen credentials (34%), vulnerability exploitation (23%), and phishing (19%).

Social engineering attacks are especially effective against SMBs, with higher rates of pretexting incidents where attackers manipulate employees into revealing sensitive information. This vulnerability possibly stems from generally lower levels of cybersecurity awareness and training in smaller organizations.

The most commonly targeted data includes internal information (sensitive plans, reports, and emails), followed by personal data and credentials. Over 90% of breached organizations were SMBs with fewer than 1,000 employees, confirming that no business is too small to become a target.

96%

of all SMB Breaches Involve Three Primary Attack Methods:

These three attack methods account for 96% of all SMB breaches, combined.

Compromised Credentials

Stolen credentials enable unauthorized access and long-term persistence.

#1: Dominant Method

Social Engineering

Phishing and manipulation tactics are highly effective against SMBs.

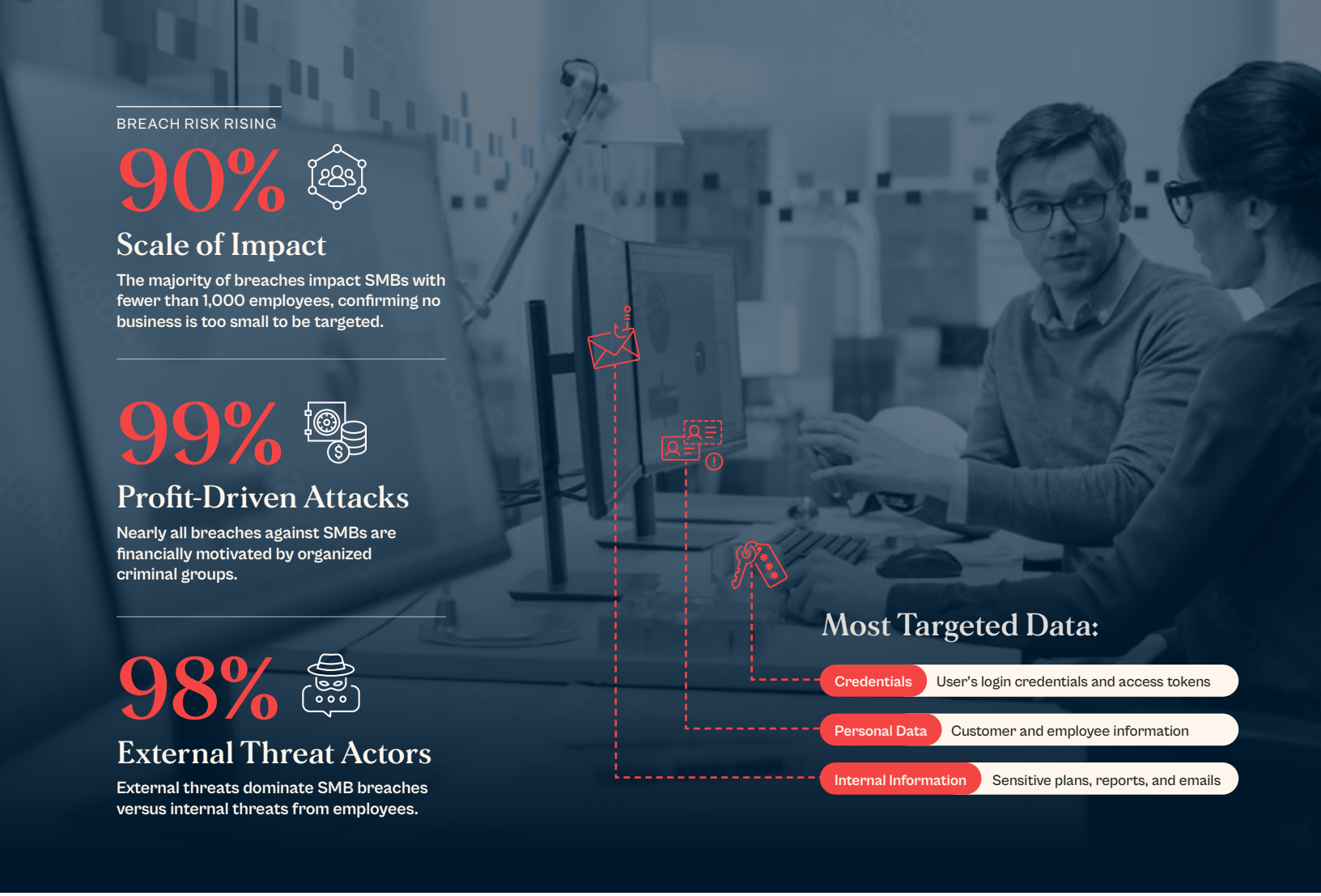
#2: Distant Second

Web Application Attacks

Vulnerabilities primarily exploited for initial access via weak or stolen credentials.

#3: Third Most Common

Malware poses a particular threat to SMBs, with ransomware leading to nearly half of all malware-related incidents.



The Financial and Operational Impact of Breaches on SMBs

Profit-driven attacks accounted for 99% of breaches against small businesses, with external threat actors carrying out 98% of these incidents. Small and medium businesses have become preferred targets because they provide reliable financial returns.

Many people wrongly assume that SMBs face less severe impacts from security breaches than larger organizations. In reality, while attackers may demand smaller ransoms from small businesses, the damage to operations, finances, and market reputation can be catastrophic. When breaches occur, SMBs suffer through extended periods of downtime that erode customer confidence and weaken their competitive position. Every business, regardless of size, plays a vital role in protecting sensitive information.

Disparities in Breach Frequency and Characteristics

According to the report, SMBs were found to have experienced breaches at nearly four times the rate of larger organizations. Among 3,049 reported incidents involving SMBs, 2,842 resulted in confirmed data disclosures. While this stark difference partially stemmed from the sheer volume of SMBs worldwide, it also pointed to their unique vulnerabilities and increasing appeal as targets.

Limited resources often prevent SMBs from implementing comprehensive security measures. With many struggling to maintain basic safeguards, such as alternatives to relying on the arduous task of restoring from backups for ransomware recovery, leaving them especially vulnerable to operational disruptions and financial losses after security incidents.

One unexpected finding showed that human errors caused only 1% of SMB breaches, compared to 18% in larger organizations. This lower rate stems from SMBs' simpler operations and smaller workforces, which naturally limit opportunities for mistakes. Despite this low error rate, social engineering attacks continue to be especially effective against these smaller organizations, as previously mentioned.

Supply Chain Implications

With a 43% surge in incidents where threat actors targeted larger organizations through their smaller business partners, the Verizon report points out SMBs' central role in supply chain attacks.

Threat actors have zeroed in on SMBs as entry points to larger enterprises, leveraging trusted business relationships to compromise systems and credentials. These vulnerabilities allow actors to move through supply chains to reach their intended targets, making SMB security essential for the entire business ecosystem.

The Role of External Threat Actors

External threat actors dominated SMB breaches with organized criminal groups emerging as the main perpetrators. These groups use ransomware and other attack methods to pursue financial gain. They employ sophisticated strategies by customizing ransom demands and specifically targeting organizations with weak security measures to exploit SMB vulnerabilities.

It was also noted that nation-state actors and internal threats are relatively rare in SMB breaches. While large organizations may face a broader range of threat actors, SMBs are predominantly targeted by financially motivated criminals seeking to maximize their return on investment.

SMB Vulnerability Analysis

Small and medium business security faces challenges with how resource constraints fundamentally shape small and medium business security today. With limited budgets and small IT teams, many organizations struggle to build strong and up-to-date cybersecurity programs. Technical expertise remains scarce, making it challenging for businesses to properly implement and maintain critical security controls.

While businesses of all sizes face similar threats, SMBs experience unique challenges. Although everyone uses comparable security tools and faces ransomware attacks, smaller organizations often lack the resources for advanced protection. As a result, they become more likely to pay a ransom when attacked.

The Human Element

Social engineering remains one of the most effective ways attackers get through the door at SMBs.

60% OVERALL HUMAN ERROR

VS

18% SOCIAL ENGINEERING

Supply Chain Risk

Threat actors increasingly target large organizations through their SMB partners, making small business security critical to supply chains integrity.

SURGE IN INCIDENTS

External threat actors dominated SMB breaches with organized criminal groups emerging as the main perpetrators.

halcyon

For small and mid-sized businesses, having a solid incident response plan and testing recovery procedures isn't a luxury–it's a must.

4X Greater Risk

Small and Medium Businesses experience breaches at four times the rate of larger organizations.

Ransomware operators continue adapting their strategies against SMBs with remarkable success. By targeting common security gaps and missing incident response plans, these groups maximize their profits through stealth and persistence. Their refined techniques let them penetrate networks extensively while staying undetected.

Building Cyber Resilience for SMBs: Key Metrics That Matter

Small and medium businesses stand at a defining moment in their cybersecurity journey. Gone are the days of simple system lockdowns. Instead, professional attackers have elevated their methods to include data theft, business disruption, and carefully calculated ransom demands. Without adequate protection, SMBs have unfortunately become attractive targets in an increasingly hostile digital landscape.

Despite these challenges, SMBs can better understand their vulnerabilities and strengthen their defenses. Organizations that understand the tools and methods used by threat actors are better positioned to protect their operations and sensitive data. Going forward, vigilance and preparation will be crucial as businesses adapt to an ever-changing security environment.

For small and mid-sized businesses, having a solid incident response plan and testing recovery procedures isn't a luxury–it's a must.

Organizations that understand the tools and methods used by threat actors are better positioned to protect their operations and sensitive data.

Here are the core metrics you should be tracking to improve your cybersecurity resilience without overcomplicating things:

Time to Detect (MTTD): How fast can you spot a cyber threat? The quicker you detect it, the less damage it can do. Regular monitoring and simple alerting tools can help cut down detection time and stop attackers early.

Time to Respond (MTTR): Once you know something's wrong, how long does it take to act? Speed matters. Practice your response plan regularly so you're not scrambling when a real attack hits.

Readiness: Is your plan actually useful in a crisis? Test it. A plan that isn't rehearsed is just wishful thinking. Run occasional simulations to keep your team sharp and improve coordination.

Employee Training: People are often the weakest link. Train your staff to spot phishing and follow basic security practices. Track who's completed training and test with fake phishing emails to see how they do.

Cyber Hygiene: Basics matter: patch your systems, scan for vulnerabilities, and fix misconfigurations. These routine tasks close easy doors that attackers love to walk through.

Know Your Risk: Understand what systems and data matter most. Regularly assess where you're vulnerable and focus protection on high-risk areas.

Vendor Risk: Your vendors can expose you too. Make sure your partners follow basic security practices and ask questions before you connect your systems to theirs.

Security Controls That Work: Firewalls, antivirus, email filters–they're only useful if they work. Check logs, monitor alerts, and don't keep paying for tools that aren't doing their job.

Backup and Recovery: Can you restore your data if something goes wrong? Test your backups. Know how long recovery takes (RTO) and how much data you could lose (RPO). Practice restores regularly.

Business Continuity: When systems go down, how do you keep running? Have a basic plan that includes worst-case scenarios and make sure everyone knows their role during a disruption.

Cyberattacks can hit any business. By tracking these core metrics and preparing ahead of time, you'll be in a much better position to detect issues early, respond fast, and recover with minimal disruption. You don't need an enterprise budget–just a plan, the right priorities, and a commitment to follow through.

The Halcyon Advantage

For small and mid-sized businesses, a ransomware attack isn't just a setback, it can be an existential threat. Many SMBs lack the resources to deploy full-scale endpoint detection and response (EDR) or extended detection and response (XDR) platforms, leaving them vulnerable to increasingly sophisticated ransomware campaigns. That's where Halcyon steps in.

Halcyon offers an economical and effective layer of protection, purpose built to stop ransomware–even in environments without existing EDR/XDR tools. Designed with simplicity and speed in mind, Halcyon adds a critical layer of ransomware-specific defense that works alongside existing security investments or as a standalone solution for organizations just beginning to mature their cybersecurity posture.

Unlike legacy tools that focus on general threats, Halcyon is laser-focused on detecting and disrupting ransomware behaviors, neutralizing attacks before encryption can occur. It's lightweight, easy to deploy, and doesn't require a dedicated security team to manage–making it ideal for resource-constrained SMBs.

With Halcyon, small businesses gain the ability to detect, contain, and recover from ransomware incidents without the need for enterprise-level security budgets or expertise–helping them stay protected, resilient, and in business.

See how Halcyon protects SMBs from disruptive ransomware attacks or talk to a Halcyon expert today to find out more.

© 2025 Halcyon. Jul 1, 2025