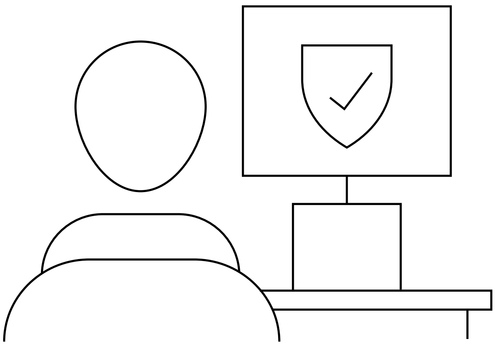
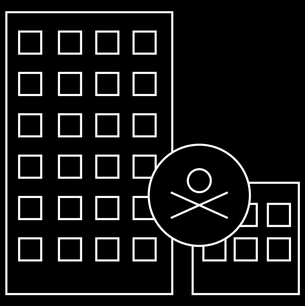
The truth behind 4 small business cybersecurity myths



The single greatest cybersecurity threat for your small business may be a false sense of security. If you underestimate risks or assume that threat actors won't target your organization, you're setting yourself up for failure.

Every year, Verizon's Data Breach Investigations Report (DBIR) analyzes incidents and breaches from around the world to provide vital cybersecurity insights to help minimize your risk and keep your business safe.

Myth 1: Attackers only target large companies.

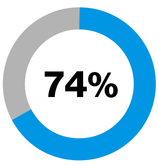


51% of small and medium businesses (SMBs) don't have cybersecurity measures in place. Of those, 59% say their business is too small to be a target.[1]

The cyberattacks that make the news tend to be ones that affect large organizations, but small businesses face constant attacks, too. The 2023 DBIR saw more breaches and incidents involving SMBs than large organizations.[2]

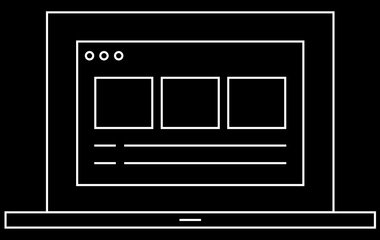
An average small business employee will experience 350% more social engineering attempts than an employee at a larger business.[3]

Myth 2: I don't have to worry about my staff.



Employees don't have to act maliciously to cause damage; one mistaken click is all it can take. The human element (Error, Privilege Misuse, Use of stolen credentials or Social Engineering) was involved in 74% of all breaches among all industry types and sizes.[4]

Myth 3: I don't need to plan—our systems are already safe.



64% of small business owners are confident they can quickly resolve any cyberattack. Yet, only 28% have a plan to respond to a cyberattack and only 26% have cyber insurance.[5]

32% of SMBs rely on free security solutions that may not deliver adequate protection.[6]

System Intrusion, Social Engineering and Basic Web Application Attacks" represented 92% of SMB breaches in the 2023 DBIR.[7]

Myth 4: Small businesses can't afford cybersecurity.

$1–2.25M

Think you can't afford cybersecurity? The truth is that you probably can't afford not to have it. According to the DBIR, the median cost per ransomware incident doubled over the past two years, with 95% of ransomware incidents involving losses between $1 and $2.25 million.[8]

$15,000–25,000

40% of small business owners expect a cyberattack to cost less than $1,000, while 60% think it would take less than three months to fully recover.[9]

Data from cyber insurance claims show breaches generally range between $15,000 to $25,000 in recovery costs. The average recovery time is 279 days.[10]

Find the right security fit.

Verizon has a range of security solutions designed for small businesses, so you can take advantage of IT expertise without the expense of a big IT staff. To learn more about how to help protect your small and medium business, visit verizon.com/dbir.

verizon

The author of this content is a paid contributor for Verizon.

1 Digital.com, 51% of small business admit to leaving customer data unsecure, March 2022.
2 Verizon 2023 Data Breach Investigations Report.
3 Barracuda, Spear-phishing report: Social engineering and growing complexity of attacks, March 2022
4 Verizon 2023 Data Breach Investigations Report.
5 CNBC | Momentive, Q3 Small Business Survey, August 2021.
6 Verizon, Is your front door open and unlocked for cyber criminals?
7 Verizon 2023 Data Breach Investigations Report.
8 Ibid.
9 Nationwide, Cyberattack recovery time and cost much higher than businesses realize, September 2022.
10 Ibid.