OpenTier SYSTEMS

Counting the Cost of Cybercrime

The Financial Fallout to Small Businesses

When a business experiences a cyberattack, the disruption can affect daily operations, employee productivity, and customer relationships—all of which have financial effects.

Rising Risks and Growing Expenses

Attackers are focusing more of their attention on small- and medium-sized businesses (SMBs), according to recent warnings from both the FBI and CISA. Successful cyberattacks can have severe financial consequences.

When it comes to the actual cost of an attack or breach, the numbers can vary, but one thing is certain: Cyberattacks are expensive relative to business size. One study of small businesses found that 40% of attacks in the US cost the victim business $25,000 or more.[1] According to IBM, a data breach costs an organization with less than 500 employees $3.31 million on average.[2]

IBM also reports that SMBs who experience data breaches are seeing their associated costs increase year over year. In fact, 57% of organizations had to increase prices to absorb the high costs.

1 Hiscox Cyber Readiness Report 2022
2 IBM Cost of a Data Breach Report 2023

The Costs of a Cyberattack

Direct financial losses: Damages from stolen funds, unauthorized transactions, or the compromise of sensitive financial information

Breach detection and forensics: Activities that enable a company to detect, investigate, assess, and audit the breach

Data recovery and restoration: The cost of recovering and restoring lost or compromised data

Loss of intellectual property: Stolen patents, engineering designs, trade secrets, copyrights, investment plans, and other IP can lead to the loss of competitive advantage

Notification and communications: Communications to customers, partners, executives, boards, other third parties, and the public

Customer care: Assistance and compensation to customers affected by the breach, such as phone support, credit monitoring, or refunds and product discounts

Business interruption: Loss of revenue and productivity due to business disruption and downtime

Reputational damage: Erosion of trust leading to loss of customers, damaged partnerships, and difficulty acquiring new customers/partnerships

Legal expenses: Costs associated with legal actions and potential lawsuits

Regulatory fines: Fines and penalties from noncompliance with applicable data protection regulations

The Good News

Small businesses don't have to just take chances, though. Steps you take today can greatly reduce the likelihood you'll sustain a breach—and if you do experience one, minimize the disruption and the cost to your bottom line.

IBM found that the more quickly companies were able to contain a breach after it was detected, the lower the breach costs they faced. This just makes sense—**the faster you detect and mitigate a termite infestation, the less damage it can do to your house.**

Interestingly, IBM also found that partnering with a provider of managed security services lowers breach costs by $73,000 on average. Organizations working with a security partner were able to identify and contain the breach faster than those going it alone.

Security Steps for Small Businesses

STEP 1

EDUCATE YOUR STAFF
Train employees in security awareness of potential threats such as phishing and social engineering, as well as best practices for protecting data.

STEP 2

BACK UP YOUR DATA
Take regular backups of business-critical data, store them securely, and test to be sure they'll work in a pinch.

STEP 3

PROTECT ACCOUNTS
Have employees use strong, unique passwords for all accounts, use multifactor authentication when possible, and consider passwordless authentication.

STEP 4

MAKE A "WHAT IF" PLAN
What if your website goes down? What if customer data is exposed? Outlining basic steps to take "just in case" can help you respond quickly and minimize potential damage.

STEP 5

ENGAGE A SECURITY PARTNER
Secure your environment with the help of a managed service provider that emphasizes strong security expertise. This should include fully managed, 24/7 monitoring, detection, and response, allowing you to focus on core business operations.

Your Partner in Protection

As a managed service provider, we provide IT and cybersecurity services to small businesses. We are backed by an elite, expert-staffed 24/7 security operations center that provides us with visibility into your environment, around-the-clock protection, and intel to drive best practices. Together, we disrupt the hacker timeline within minutes—stopping breaches before they escalate into severe financial setbacks.

Harness our experience protecting businesses like yours — contact us today.