LESSONS LEARNED FROM DATA BREACHES: WHAT YOU NEED TO KNOW.

No Organization Is Immune. Cybersecurity Demands a Proactive Strategy for All.

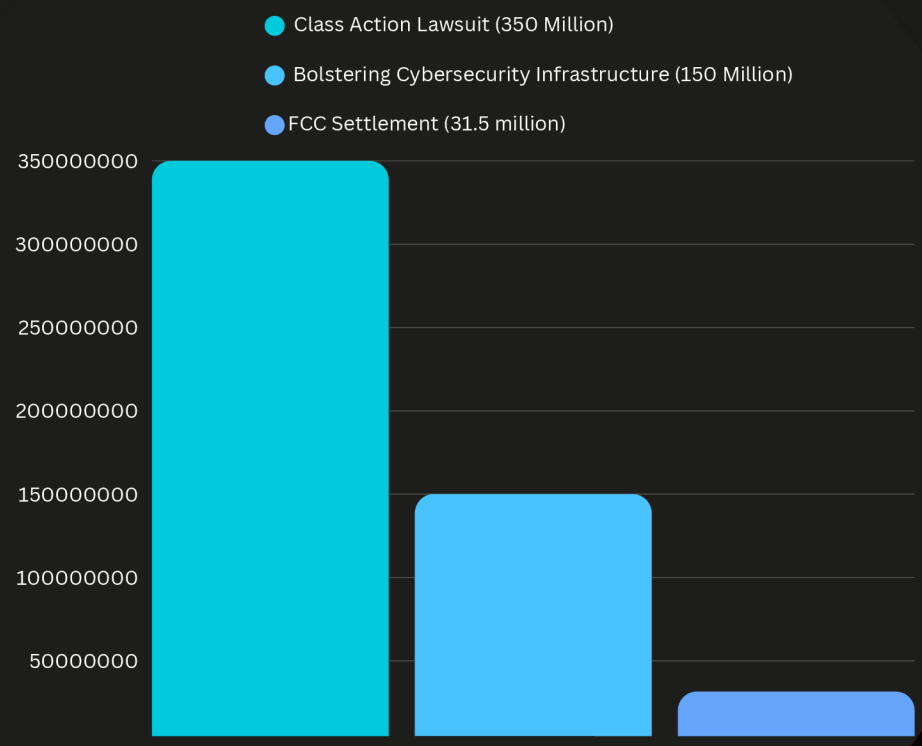
xentexsolutions.com

CYBERSECURITY MUST BE A BUSINESS-WIDE PRIORITY

T-Mobile's 2021 data breach, which exposed the personal information of 37 million customer accounts, serves as a valuable lesson for businesses of all sizes, especially small and medium-sized businesses (SMBs). While T-Mobile is a telecom giant with vast resources, the breach highlights how even the biggest companies can be vulnerable. It's also a wake-up call for SMBs about why cybersecurity needs to be a top priority.

Xentex Solutions dives into the key lessons learned from data breaches and explores how organizations can apply these insights to strengthen their security posture.

FINANCIAL IMPACT OF T-MOBILE DATA BREACH: TOTAL LOSS BREAKDOWN



A data breach of this scale can deeply affect an organization, jeopardizing its stability and growth potential.

HIDDEN COSTS OF A SECURITY BREACH

- Lost Customer Trust
- Weakened Brand
- Higher Cyber Insurance Premiums
- Lost Productivity

When a security breach occurs, the financial fallout is just the beginning. The real damage often lies in the hidden costs.

IBM's 2023 Cost of a Data Breach Report found that nearly 40% of the average cost of a breach comes from lost business. This includes customers leaving, damage to the company's reputation, and downtime that impacts critical systems and disrupts productivity.

COMMON INFRASTRUCTURE WEAKNESSES THAT LEAVE YOU EXPOSED.

OUTDATED HARDWARE IS A SILENT THREAT

Routers now account for more than 50% of the most vulnerable devices in organizations of all sizes, primarily because many of these devices are no longer supported by their manufacturers and do not receive critical security updates.

UNSEGMENTED NETWORKS LET ATTACKS SPREAD FAST

Only 19% of SMBs use proper network segmentation, giving intruders a free pass to move laterally once they're in. And only 38% of mid-market and enterprise organizations implement effective network segmentation

MISCONFIGURED FIREWALLS LEAVE YOU EXPOSED

30% of breaches involve firewall misconfigurations that create hidden openings in your network perimeter. Without regular audits, these gaps go unnoticed until it's too late.

COMMON INFRASTRUCTURE WEAKNESSES THAT LEAVE YOU EXPOSED.

REMOTE ACCESS IS OFTEN WIDE OPEN

68% of companies allow unrestricted RDP access from the internet — prime hunting ground for malicious hackers. Lock it down.

IOT DEVICES ARE OFTEN BACKDOORS

57% of IoT devices are exposed to medium- or high-severity threats. Without proper safeguards, they become open doors to your technology ecosystem.

UNPATCHED SOFTWARE OPENS THE DOOR FOR EXPLOITS

Unpatched software is involved in 60% of cyberattacks, with attackers exploiting known vulnerabilities to gain access

UNSECURED ENDPOINTS EXPOSE YOUR NETWORK AND DATA

Endpoints like laptops, desktops, and mobile devices are prime targets. 70% of successful breaches originate at the endpoint. Without advanced protection and monitoring, every device is a potential entry point for hackers.

CYBERCRIMINALS DON'T CARE HOW BIG YOU ARE.

THEY CARE HOW VULNERABLE YOU ARE.

Threats evolve.
So should your security.

Most SMBs think they're too small to be targeted. That's exactly why they are.

- ✓ Proactively monitor your network activity.
- ✓ Patch vulnerabilities before they're exploited.
- ✓ Endpoint threat detection and response.
- ✓ Segment your network to contain breaches.
- ✓ Run regular vulnerability assessments.

These are just the basics.
Real protection goes much deeper.

Just as you're dedicated to your business, Xentex Solutions is dedicated to making cybersecurity work for you efficiently, securely, and with the expertise to keep your business running smoothly.

Contact Xentex Solutions today to learn how we can help you protect what's most important!

contact@xentexsolutions.com
P: 561-973-0302

xentexsolutions.com