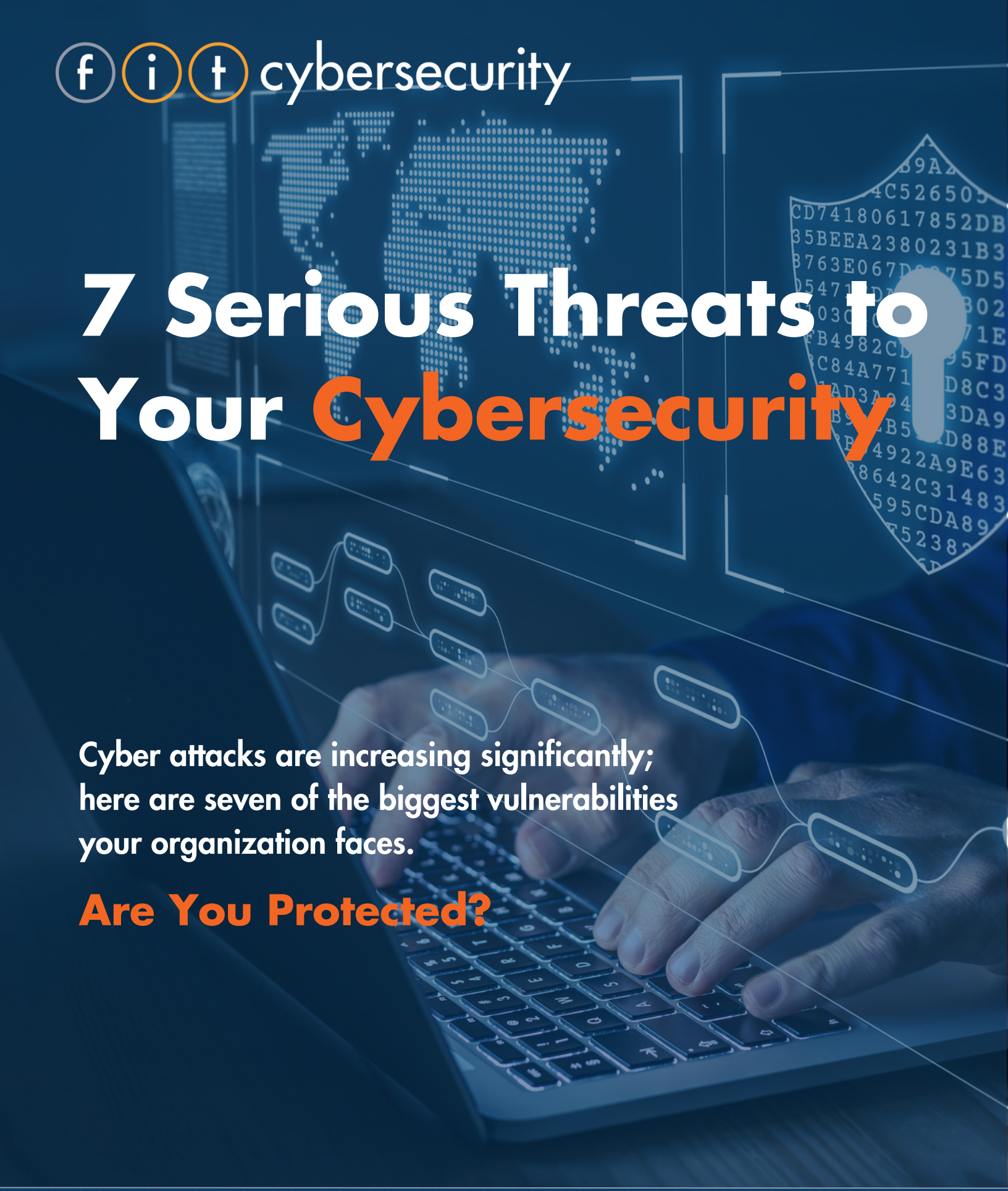
fit cybersecurity

7 Serious Threats to Your Cybersecurity



Cyber attacks are increasing significantly; here are seven of the biggest vulnerabilities your organization faces.

Are You Protected?

www.FITsolutions.biz info@FITsolutions.biz 888-339-5694

fit cybersecurity

Impersonation Attacks

One of the most successful strategies in social engineering is when a bad actor impersonates someone within your company. In a recent study, 41% of users who clicked on a phishing email did so because it appeared to have come from a senior executive. By posing as the IT Director, the CEO, or someone else with authority, a criminal can gain access to your network, your payroll system, or your clients' data. How might your business be vulnerable to impersonation attacks?

1. Lack of Multi-Factor Authentication

Do you have MFA enabled on your business email? If not, your employees' email accounts may be vulnerable to attack by bad actors if their credentials have been sold on the Dark Web.

2. No Email Filtering System

Tools like Mimecast do more than catch malware; they can filter impersonation emails by quickly and thoroughly scanning emails for anomalies in the domain, header, sender, and content.

3. SIEM But No Monitoring

You may already be using a SIEM (Security Information & Event Management) tool, which consolidates real-time data from across your network into security alerts. But if your security team only works 9 – 5, who's monitoring and responding to those alerts? To be effective, you need 24/7 monitoring of your SIEM tool.

888-339-5694

fit cybersecurity

of ransomware attacks targeted businesses with under $50 million in revenue

of businesses targeted in 2021 paid a ransom

Businesses that paid the ransom recovered only 65% of their data

Ransomware

Globally, there were 304 million ransomware attacks in 2020. In 2021, we hit 304 million in the first six months! Forbes reported that 80% of the organizations they surveyed were hit with ransomware in 2021. Ransomware is the third most used form of cyber attacks, and the cost of a ransomware breach averaged $4.62 million in 2021, not counting the ransom itself. Clearly, this is not a threat to be taken lightly.

4. No Software Restriction Policy

A Group Policy Object provides a centralized way to control advanced settings across your users' computers. Without it, each device can have different security settings, posing a threat to your network security. Workstations that have not had AutoPlay, AutoRun or unauthorized extensions disabled via GPO may be susceptible to ransomware attacks.

5. No Endpoint Protection

A simple firewall isn't enough to protect your environment; if a bad actor or malware gets past those basic defenses, each device in your network is vulnerable. Endpoint protection like Sophos Intercept X secures each device from exploitation, disabling file execution of email attachments or quarantining attachments through the spam filter.

fit cybersecurity

Social Engineering

As much as 98% of cyber attacks rely on social engineering—when a criminal tricks someone into giving up valuable information—and over 70% of all breaches can be traced back to successful social engineering tactics. Why are these numbers so high?

6. Lack of Regular Awareness Training

Your team is the weakest link in your security. A study from Stanford University found that 88% of all breaches are caused by human error. Annual training isn't enough; we're all busy and distracted, and criminals are testing new tactics every day.

7. No Wire Transfer Policies

One of the worst breaches we've seen happened when a criminal had gained access to email systems, and waited months for the perfect opportunity. He intervened in an email exchange about a legal settlement, sent new wire transfer information, and made off with millions. This could have been prevented if the organization had a verbal confirmation wire transfer policy in place: a hard-and-fast rule that no wire transfers should be sent without a verbal confirmation—not just email.

Each of these could pose a serious cybersecurity risk to your business. Talk with our team today to get a free evaluation of your risk profile and recommendations on how to increase your defenses against a cyber attack.

Schedule Your Free Consultation Today

888-339-5694