CYBRID

YOU ARE GOING TO GET HACKED

According to a recent Cisco study, 60% of all small-to-mid-sized businesses that are breached go out of business within one year. Being proactive and not taking your technology's security for granted will prevent you from becoming a statistic.

Introduction

Few illegal activities are on the rise more than cybercrime. Never before have businesses been more prone to security breaches and cyber-attacks and less prepared. We have become technology-dependent, and as teams grow, so do software solutions and infrastructure. With more potential areas open to exposure, cyber breaches in small-to-medium businesses are at an all-time high and yet, according to Hiscox's Cyber Readiness report, **73% of businesses do not have adequate security measures, systems and processes.**

27BN

lost annually due to cyber attacks. Source: gov.uk

46%

of businesses reported a cyber attack in the last 12 months. Source: gov.uk

Next: The Rise of Cybercrime

The Rise of Cybercrime

The same report by Hiscox stated that one small business in the UK is **successfully hacked every 19 seconds**. Depending on the intent of the hacker, a business may have data stolen, experience significant and costly downtime, or succumb to complete system destruction.

This is precisely what happened in the case of GPS wearables company, Garmin. On July 23 2020, Garmin users took to social media to express concern over inaccessible website features. Four days later, Garmin released an official statement confirming that a cyberattack had taken place - although users were assured that no PII (personal identifying information) was compromised. Hackers deployed a ransomware tool that encrypted key data on the company's digital infrastructure. Website functions, customer support, and user applications were all affected and rendered programs useless until decrypted. The hacking organization then demanded a fee for the decryption key. In the case of Garmin, although not verified, it is believed the $10 million ransom was paid.

Cybercrime is not just reserved for big businesses. Organizations of every size are vulnerable to attack. Cybercriminals are willing to work relentlessly, 24/7, using technology that finds the weakness in your security to expose it via a breach. It's also not only ransomware that can have devastating financial consequences - according to Datto, on average, **downtime costs 23X more than the ransom requested**.

Next: Steps To Preventing Cybercrime

Steps To Prevent Cybercrime

What can your company do to avoid a fate similar to Garmin? Defending yourself against cybercrime is nearly impossible to do alone, especially if you rely on any technology to conduct your business. The perpetrators are professionals and they are hard to counteract with amateur efforts. But there are some things you can implement to guard yourself against and minimize damage in the event of an attack.

Find the right technology partner

Find the right IT partner for you, who doesn't just help manage and procure your IT equipment, but proactively plans and initiates conversations around security. With the right partner, you'll feel safer, and be safer from attacks in the future.

You need a **layered defence strategy** - separate backups, vulnerability assessments, patch management, remote management, anti-virus, and anti-ransomware - all of which requires a technology partner to learn and maintain all of those applications.

But what happens when even those methods fail, and a ransomware attack is upon you? At that time, you have a disaster on your hands, and your last line of defence is your disaster recovery plan. **A technology partner will keep your data protected in real-time**. If – and when – a cyberattack makes it past your defences, your data can be recovered in seconds with just a few clicks.

Achieve a Cyber Essentials Certification

Cyber Essentials is a UK Government-backed scheme that aims to reduce cyber vulnerability. When implemented correctly with the help of a technology partner, the security controls outlined should prevent 80% of cyber-attacks. Not only does it protect your business from cybercrime, but it also demonstrates to your customers and supply chain that you have considered security controls and are working in a safe and secure environment. **If your company is looking to secure public sector contracts, it is absolutely essential that you have the Cyber Essentials certification.**

Continues: Steps To Preventing Cybercrime

3 Train Team Members

Making security an important discussion in your business is the first step to highlighting its importance and getting everyone on the same page. **Cybercrime prevention for businesses is a joint effort** and every team member should recognise why they should be on board with newly implemented policies and procedures.

4 Implement Cyber AI

Cyber AI systems like Darktrace learn the unique 'DNA' of your organisation and can detect cyber threats that may otherwise be missed. The technology knows exactly what action to take, at the right time to neutralize an advanced attack, and **delivers 24/7 protection when your teams cannot respond fast enough**. Its technology is powerful enough to identify a diverse range of threats at their earliest stages – including insider attacks, latent vulnerabilities, cloud-based threats and even state-sponsored espionage.

For many companies without dedicated security departments or a technology partner, it's not a matter of if, but when. You are going to get hacked.

As a business owner or decision-maker, the steps you take to protect your business from cybercrime are critical. Get in touch to arrange your free cybersecurity assessment and defend your business from insider threat, IoT hacks, malware, misconfigurations, data leakage and unusual behaviours.

CYBRID
Technology Solutions Partner

Simplifying the complex.

E: enquiries@cybrid.solutions **W:** cybrid.solutions
T: 0345 567 0006