How Do You Manage Cybersecurity With Employees Across the Globe? Here's Your Answer.

Opinions expressed by *Entrepreneur* contributors are their own.

Cybersecurity is a $60 billion industry, and it continues to grow year over year. Most companies are careful to take extreme precautions to keep their sensitive data, and that of their employees, protected. But when you combine the rise of remote work over the last decade with a global pandemic, it throws a real monkey wrench into an otherwise well-oiled machine.

According to Statista, data breaches within the U.S. (where they also happen to be the most frequent and most expensive) cost an average of $8.6 million — enough to bring your business to a screeching halt. So, how do you keep your proprietary and private information safe? We'll find out, but first, why are remote companies much more susceptible to cybersecurity threats and breaches?

- **Unsecured Wi-Fi.** When remote employees work from anywhere, they really do work from *anywhere*. That might mean a coworking space with secure Wi-Fi, but it might also mean a coffee shop, an airport or the gym. Whenever your company's data is accessed over one of these networks, it's at risk.
- **Personal hardware.** It's possible you've provided your employees with company-owned laptops and secure server access, but it's equally as likely that they're doing at

least some (if not all) of their work from their personal devices. This also means that a personal laptop, which is far more likely to be left unlocked and in the open, can be compromised.
- **Inadequate training.** If your remote employees haven't gone through cybersecurity training, add it to your to-do list, stat. Go over VPNs, authorized use of personal devices, password management and data encryption.

According to *Business Tech Weekly*, 81% of CIOs said their company had fallen victim to a Wi-Fi-related security breach in the last year (with 62% of them originating in cafes or coffee shops). So how do you keep your remote team from becoming a statistic?

Related: Protect Your Business by Becoming a Cybersecurity Analyst

Create a cybersecurity response plan

One weak password could be all that's standing between your remote company and a serious cyber breach. That's why it's critical to have a cybersecurity response plan in place. Your plan should cover, at minimum, all the basic information from your cybersecurity training, plus how to identify scams and phishing attempts, and what employees should do if and when a breach is suspected.

Be sure your action plan is comprehensive, is shared across the organization and is quickly accessible when needed. Institute a cybersecurity "chain of command" so employees know where to turn if they believe they're involved in a cybersecurity incident.

Adopt a password management system

What do your anniversary, your mother's maiden name and your kids' birthdays all have in common? They're all terrible passwords. And yet, they're some of the most commonly used. Instead of leaving it up to employees, implement a password management system that will ensure your team has access to the software, tools and resources they need while keeping your information protected. In addition to a password management system, remind your employees when choosing passwords to:

- Use the system's recommended password or choose a password that is unique and doesn't include known personal information
- Avoid using the same password across multiple platforms
- Change passwords on a regular basis

Related: **How to Keep Your Company Safe From Cyber Attacks**

Use multi-factor authentication

Multi-factor authentication (MFA) requires verification from your employees to access sensitive or restricted information. Essentially, they must provide proof that they are who they say they are. Types of MFA include:

- PINs or verification codes (often sent via SMS)
- Security questions
- Real-time access requests (an authorized user approves access when requested)
- Biometrics, including fingerprints, retinal or face scans
- Hardware like key fobs or badges that must be scanned before accessing protected information

MFA is evolving rapidly and breaking into new technologies, so make sure you work with a trusted professional to choose the types of multi-factor authentication for your remote team.

Make common sense a little more common

Hiring a cybersecurity pro can get pricey (though it’s a worthwhile investment), but there are small steps every remote employee can and should be taking, especially if you need to ensure your data is protected while you put a cybersecurity plan in place. Starting now, make sure every remote employee takes the following actions:

- Ensure personal laptops are password-protected and never left unattended and unlocked
- Turn on your firewall
- Enable encrypted backups
- Use a secure internet connection when working in a public place, or if that isn’t possible, use a VPN

Whether you’re new to managing a remote team or an old pro, the need for increased cybersecurity is constantly growing. And when your employees are working from home, working while traveling or working from far-flung locations, it’s easy for a small chink in the armor to result in a fatal blow. Keep the above tips in mind when creating your cybersecurity response plan and ensure your employees – and your company’s most sensitive information – are constantly protected.

https://www.entrepreneur.com/article/430895