The Workforce is Shrinking…Your Security Shouldn't

If you are struggling to find cybersecurity professionals, you are not alone. A worldwide shortage of professionals in this industry continues to grow. Even as more people than ever enter the workforce, demand rapidly exceeds availability. However, this does not mean your company can get lax regarding security. As the employee shortage grows, so does the frequency of cyberattacks.

Problems in the Cybersecurity Workforce

A new study of the cybersecurity workforce shows that the workforce is at an all-time high but is still highly short-staffed. There are an estimated 4.7 million cybersecurity professionals worldwide, but there is a global shortage of around 3.4 million workers. This means that the industry is only operating at about 58% capacity, which leaves many companies, governments, and other organizations vulnerable to cyberattacks.

There are more than 700,000 unfilled cybersecurity jobs in the United States. Companies are desperate for employees, but the extensive knowledge required to be in this field and retention cost limit success. The median salary for a cybersecurity professional in the United States is around $135,000, so small businesses are especially limited in hiring talent. Although many people are getting into the field because of these high salary potentials, there are not enough people with adequate credentials to fill these roles.

Why Security Must Stay a Top Priority

You might be thinking that paying for cybersecurity does not justify the benefits. Here are some statistics that might change your mind:

- So far, in 2022, the total cost of cyberattacks worldwide is over $6 trillion. This number will increase to $10 trillion per year by 2025.
- A ransomware attack happens every 14 seconds.
- Small businesses, on average, spend less than $500 each year on cybersecurity, but one in ten small businesses will suffer a cyberattack.
- According to Juniper Research, the United States will become the target of more than 50% of worldwide cybercrime in the next five years.
- 95% of security breaches happen because of human error.

The world has become increasingly digital over the past few decades. Unfortunately, cybercriminals have become highly advanced, but cybersecurity has yet to respond. Rather than being proactive, many companies are reactive and attempt to fix problems after they occur. As criminals get even more advanced, this will no longer be an option–companies must implement a complete cybersecurity strategy if they hope to survive the next few years.

Unfortunately, in times of high inflation, where small businesses are already struggling to get new clients and pay their staff, a cyberattack could be the thing that ends their business. Although it might be challenging to find money in a monthly or annual budget to implement cybersecurity measures, these will pay off in the long run. Apart from implementing automated security, companies should teach employees about phishing and other common threats that can be easily avoided.

How to Fix These Problems

Instead of hoping that millions of tech workers appear out of thin air, companies need to begin to rely on automation in cybersecurity. Securitech180 is a revolutionary tool that offers advanced protection against advanced threats. It is a first-of-its-kind automated response platform that provides cyber security for all devices on a network. After an easy installation, ST180 blocks cyberattacks before they ever reach your network.

ST180 ships as a pre-configured plug-in appliance. It then generates network and threat intelligence and requires zero management from your team. ST180 is constantly evolving and learning from the most current global sources to find and block threats as they occur. Every 180 seconds, Securitech identifies, isolates, and immobilizes any threats on your network.

Automated cybersecurity is the future, as it does not rely on humans, which involves human error, to respond to attacks. It is much more cost-effective to use automated security rather than pay staff around the clock to monitor the network, who might still miss something. As we have seen, getting this staff in the first place is almost impossible. Automation helps teams manage and respond to the ever-increasing number of threats.

Bottom Line

The government has many resources for small businesses that need help implementing a cybersecurity strategy. They are also beginning to roll out several requirements for small and large companies to protect consumer data and report cyberattacks. You should expect these requirements to become more strict in the coming years as cyberattacks become more common and staffing shortages in the industry become more detrimental.

To stay ahead of these attacks, implement tools like Securitech180, which can save massive amounts of money from cyberattacks. Automation using artificial intelligence and machine learning is the only way to move forward in this field. It is more effective, efficient, and accessible than anything else on the market. If you are interested in learning more about the state-of-the-art system, contact us or book a demo.