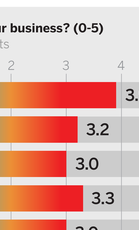
THE 2020 THREAT LANDSCAPE: HOW PREPARED ARE YOU?

With the huge surge of remote workers, IT teams are under severe pressure to make sure their systems are safe from attack. The level of cyber threat has also escalated, with attackers adding new techniques and tactics to their arsenal by the day.

Many of these threats are unknown, can prove challenging to detect and can have severe implications for your business – an hour of shutdown could be costly, a day could be catastrophic.

In a recent survey, produced in partnership with WatchGuard, *SC Media UK* asked what you think are the major cyber threats to your business and whether you feel these threats will increase over the next 12 months. The survey also investigates if you are confident that you have the necessary solutions, skills and support in place to protect your business against cyber attacks, both now and in the future.

The bad news is that the threat is real. **Almost half of you had experienced a cyber attack in the past 12 months.** And a somewhat alarming 11% were unsure whether you had experienced an attack or not.



A huge majority of you felt that cyber security threats are likely to increase over the next 12 months.

PHISHING SCAMS

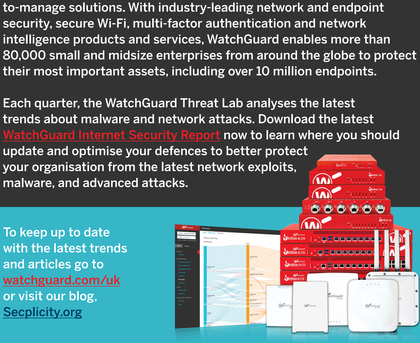
You considered phishing to be the greatest cyber threat to your business. Authentication attacks and stolen credentials were considered as the second greatest cyber threat to your business.

What is the greatest cyber threat to your business? (0-5)
Average ratings among the 230 respondents

TIME AND BUDGET CONSTRAINTS

You said the biggest potential barriers to improving your organisation's security were not being given enough time to work on improved safety measures and not being given the required money to implement them.

What is the biggest barrier to improving your organisation's security? (0-5) Average ratings among the 230 respondents



HOW MUCH IS YOUR BUSINESS AT RISK?

In times of global challenges, geopolitical uncertainty and disruption to traditional working practices, cyber criminals find new and inventive ways to scam people and businesses when they are at their most vulnerable.

These stats reveal that if you haven't already experienced a cyber attack in the past 12 months, then many of you are expecting cyber security threats to your business to increase over the next year. You have identified the risks but are concerned that internal barriers are preventing you from protecting your organisation from very real threats.

The good news is that a healthy majority of you felt more confident that you have the tools and resources to secure your remote workers and protect your business.

But you were slightly less confident that you have the right skills and resources in-house to protect your business against a cyber attack.

WHAT'S THE ANSWER?

While cyber criminals are aiming to profit from uncertain and challenging times, cyber security professionals are working non-stop to halt them. Although this has brought out the worst in threat actors and hacking groups, help is available.

For more than 20 years, WatchGuard has pioneered cutting-edge cyber security technology and delivered it as easy-to-deploy and easy-to-manage solutions. With industry-leading network and endpoint security, secure Wi-Fi, multi-factor authentication and network intelligence products and services, WatchGuard enables more than 80,000 small and midsize enterprises from around the globe to protect their most important assets, including over 10 million endpoints.

Each quarter, the WatchGuard Threat Lab analyses the latest trends about malware and network attacks. Download the latest WatchGuard Internet Security Report now to learn where you should update and optimise your defences to better protect your organisation from the latest network exploits, malware, and advanced attacks.

To keep up to date with the latest trends and articles go to watchguard.com/uk or visit our blog, Secplicity.org