CYBER SECURITY IS A JOURNEY NOT A DESTINATION...

IN BOTH OUR PERSONAL AND PROFESSIONAL LIVES, WE INVEST TIME AND MONEY IN PROTECTING OURSELVES IN SO MANY WAYS WITH HOME, MOTOR AND LIABILITY INSURANCES, BUT THIS ATTITUDE IS RARELY BEING DEPLOYED TO PROTECT AGAINST CYBERCRIME.

THIS INCREASINGLY LUCRATIVE BUSINESS NETS CRIMINALS MILLIONS EACH YEAR, WITH INCENTIVES RISING.

ONLY 55% OF WEBSITES ARE TRUSTWORTHY

THE UK GOVERNMENT ESTIMATES THAT CYBERCRIME COSTS AROUND £27 BILLION

30% OF INTERNET USERS ACCESS DANGEROUS WEBSITES

ONLY 28% OF MOBILE PHONE APPS ARE TRUSTWORTHY

37 MILLION VIRUSES WERE DETECTED BY DELL IN 2014, ALMOST DOUBLE THE AMOUNT COMPARED TO 2013

Perhaps it is the fear of the unknown that is being overlooked and the devastating effects are never appreciated until a cyber-attack occurs. We mustn't forget that cybercrime could be the assassin that kills your business, so it needs to be taken seriously. The good news is that putting the right protection and appropriate education in place is easy to do.

You and your staff are too busy to spend the working day thinking about security threats so implementing a solution that works hard for you in the background is the right business choice. Attribute a value to your company's data – once the worth is realised, protecting it will seem obvious and cost effective. The UK government estimates that cybercrime costs around £27 billion per annum. While the public and the government take their fair share of incidents, almost 80% (£21 billion) of this financial damage is attributed to attacks on the business community.

This notion is backed by the new recommendations from the Guernsey Financial Services Commission that businesses are expected to conduct themselves responsibly in the cyber environment, which primarily means protection and education. Wider than our individual businesses, this is to ensure the Channel Islands remain a safe and trusted jurisdiction in which to do business. The new EU data protection legislation also states any companies doing business in the EU will face a potential fine of up to 4% of global turnover for data breaches.

Is it on your boardroom agenda?

The threat of cybercrime is real and must be taken seriously at boardroom level. Industry research suggests that many boards lack adequate expertise and understanding of cyber risks. Cybercrime can seriously damage a business' bottom line and brand reputation in an instant, making an attack hard to recover from. Essentially, the financial future of a company and its customers can hinge upon the security of the information stored. Not forgetting the personal risk directors run if their businesses are not adequately protected.

Is the threat real?

Contrary to popular belief, it is certainly not just large multinationals who are being targeted here. SMBs are because their modest security budgets make them more accessible and through these SMBs the supply chain of larger companies can be affected which, in turn, makes them vulnerable to extortion.

There is also a perception within the business community that because of our geographical location, we are immune to a lot of security threats. In reality, as the Channel Islands are such global players in financial services, e-gambling etc. it actually means we are a direct target. Cyber security needs to be prioritised because it can seriously threaten the survival of businesses. The Channel Islands are a great place to do business and everyone must be vigilant of cybercrime to ensure we remain a trusted jurisdiction.

If you are not prepared to perform an audit on your internet security, there are many criminals who will. Cybercrime is now part of organised crime and age-old crimes including blackmail, sabotage and terrorism come as standard. Trends will shift so that cyber security becomes as routine as locking the doors to our offices and setting alarms.

Education is vital

Those businesses which have adopted a culture shift to educate their staff and implement security policies are king.

Whilst the appropriate technology should be put in place which can significantly improve security, there will always be a human element to cybercrime so education for everyone is key. Threats can come from anywhere and are most often a result of staff innocently clicking links, opening emails or using unprotected Wi-Fi or even business partners not having appropriate protection and sending emails to you. A complete lockdown is not required and businesses can still offer their employees, partners and suppliers the benefits of modern flexible working, providing appropriate protection is in place.

The right education for staff raises their awareness to spot potential threats, which is not laborious or time consuming.

Get on-board

Security-as-a-service is the most cost-effective way to protect your business and the most proactive. Security-as-a-service also allows enterprises to access security services that are robust, scalable and cost effective. Unlike an insurance that only pays out if something goes wrong, security-as-a service is a constant, proactive protection for your business and staff.

Whilst everything can be taken care of, it is important to understand that cyber security is a journey and there is no quick and easy one-stop-shop solution. Threats evolve, therefore so must the protection we provide. This is achieved with a combination of software, hardware and industry knowledge that we instantly pass on to security-as-a-service clients.

It is no longer just a case of 'getting ahead' in business, good cyber security is a minimum requirement in many jurisdictions around the world. Cyber security does need to be taken seriously in order to future proof your business.

Perhaps it's time to start your cyber security journey?

For a free no obligation consultation please contact a member of the Resolution IT team on 01481 267338 or info@resolution-it.co.uk

RESOLUTION IT