How to make cyber security a solid part of your business's culture

DRAGON

Cyber crime is the number one threat to businesses everywhere.

Everyone knows about the risks, but every day thousands of people click on infected links, give out their bank account details to fraudsters and leave their mobile phones on trains.

Big name companies that we'd all assume should know better, end up leaking confidential records or paying out ransoms to hackers. Even the state of Florida has fallen prey to three huge ransomware attacks so far this year, and let's not forget the Wannacry virus that spread through the NHS's computer systems in 2017.

The media bombards us with stories about cybercrime and terrorist attacks. We're living in constant fear of crazy politicians with access to big red buttons. Our brains are wired to technology and anxiety levels are at an all-time high.
So why, in a world that's so obsessed with threats, do we continue to make these silly mistakes?

Part of the problem is that we're all working too hard. All this constant connectivity is great, but it's harder to find the "off" button when you can work around the clock from anywhere in the world. Tired people make mistakes, which is why air traffic controllers are only allowed to work for chunks of an hour and a half at a time. Another reason for this apparent failure to take internet security safely is good old-fashioned apathy.

Companies that get cyber security right are the ones that embed it into their culture. Like turning the lights off at night or filling up the tea urn in the morning, it should become a routine part of your daily way of life. When the right systems and procedures are in place and adequate training is provided, making the right choices just becomes second nature.

Creating a Culture of Security

All cultures need time to grow. It's not something that's going to happen overnight, but if you invest in the right tools and lead by example, you'll soon be able to transform your organisation and create a secure, panic free environment.

1. Willingness to change

Successful organisations understand the importance of responding to what's going on in the world and aren't afraid of new technology.

2. Strong leadership

If staff see their managers sharing passwords, the message is that it's ok to be lax about security. A solid security culture starts at the top and should be embedded in everything you do.

3. Celebrating success

For people to invest their time and effort, they need to see that it's worthwhile. Good cyber security companies will be able to provide you with reports about suspicious activity and potential breaches. Sharing these with staff will help them understand they're making a difference.

4. Return on investment

Cyber security services are all about lowering vulnerabilities and protecting data, but not all offerings are created equal. Selecting the right provider will enable you to show stakeholders you're spending money wisely.

Why do organisations need a security culture? Isn't software enough?

How many times have you heard people making excuses about "computer errors"? It's the go-to response when payments are missed, astronomical bank charges are requested, and files mysteriously go bump in the night. But the reality is, computers don't make mistakes - they do exactly what we tell them to do.

Humans, on the other hand? We're always the weakest link - too much stress, a few drinks after hours and rushing to make it out the door by 5pm can all make people scatty.

According to a 2019 survey conducted by Censuswide, 89% of surveyed organisations in the UK said they had suffered some kind of security breach - of which a staggering 63% had been down to user error.

That's why the phrase "you're only human" exists. We're not super infallible beings; we slip up from time to time. And when we do, the consequences can be dire.

Embedding security culture into your organisation is all about minimising those mistakes and providing humans with a framework that helps them make good decisions.

5 steps to creating a sustainable security culture

1. Instil a sense of ownership

It's common for people to think that cyber security is someone else's problem: "No, it's not up to me, it's the IT guy's job!" While it's true that your IT provider should be taking overall responsibility for security tech and monitoring your system for suspicious behaviour, that doesn't mean the buck stops with them. A security culture is for everyone and adhering to the rules should be non-negotiable.

2. Provide the right training

As a general rule, people want to do the right thing - the vast majority of in-house data breaches have nothing to do with malicious intent, but lack of education. Simply sticking posters up around the office isn't enough - they'll become part of the furniture and get ignored. It's important to assess everyone's awareness of internet security and start with the very basics if necessary.

3.Use mistakes as an opportunity to grow

Even the most organised organisations have their off days. Instead of trying to brush things under the carpet, use slip ups as a learning opportunity and build them into your risk assessment. No need to name and shame the individuals involved, but things like lost mobiles and accidental link clicks can become great teaching moments.

4. Implement a Secure Development Lifecycle (SDL)

An SDL is a set of processes and activities that organisations need to perform to keep their data and systems safe. It includes risk assessments and threat modelling, security patches, password management, upgrades and ongoing monitoring. If this all sounds like just another onerous task, the good news is that a reliable IT service provider will be more than happy to talk you through it.

5. Reward good behaviour

It's great if you're in a position to offer perks for doing cyber security training and following good practice, but that's not always possible. A simple thank you never goes amiss. And employees who go above and beyond to make cyber security a priority can perhaps be given roles like "security ambassador" or be featured in your company newsletter.

Creating a culture of cyber security is good for everyone. It provides team members with opportunities to grow and learn. And gives both employees and customers peace of mind that their valuable data is being taken care of.

Where are you right now?

An appraisal of your current IT set up and staff awareness will help you focus on what needs to be done. Contact us today to arrange a no-obligation assessment.

Even if you've never given cybercrime more than a passing thought, the fact that you're reading this right now means you're on the way to creating a culture of security.

Even small changes, like ensuring your team do some basic training on how to recognise a phishing email, can go a really long way towards making your business more secure. It's going to take time for it all to filter through and become second nature, but with the right procedures and attitudes in place, you'll get there.

For proven, trusted IT systems support to keep your business trading profitably

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com