engage CUSTOMER

wavex
EXPERIENCE EXCELLENCE

BEST PRACTICES FOR MAKING CYBER SECURITY WORK

For many organisations their approach to cyber security is very much a reactive one — they've experienced a breach or attack, or an organisation in the same market space has been a victim, and up until then their attitude has been 'it hasn't happened to us'. However, with the number of cyber attacks increasing exponentially — PwC reported a 38% increase in detected information security incidents in 2015 in its Global State of Information Security report — there's increased focus on mitigating risk and protecting valuable data.

While the tides have certainly changed regarding acceptance that cyber-attacks are almost inevitable, security is at the top of almost every organisation's agenda, and budgets have become larger, there is still a lot more that needs to be done for companies to take a truly proactive approach to cyber security.

One of the key elements in this fight is buy-in from C-level. In the past, cyber security was seen merely as an IT issue. IT engineers were responsible for patching, maintaining the company firewall and ensuring software was up to date. Now, however, as a result of the scale and sophistication of attacks and the methods that are being used (from brute force attacks and malware, to social engineering) cyber security is a company-wide endeavour that must be championed from the top down. This is especially evident in the fact that budgets are increasing dramatically, too. In fact, in the UK they doubled in 2015.

But what other aspects should a business look at to help guard against cyber attacks, beyond firewalls and anti-virus software?

Company-wide user education

It's not enough to have a set of best practices as part of a cyber security strategy without communicating them to the entire organisation. Also, educating users is playing an ever more important role in cyber security, and should focus on the dangers and risk of cyber attacks, the impact of their actions and what they can do to mitigate those risks. According to the Information Commissioner's Office (ICO), human error accounts for the majority of data breaches, whether that's through social engineering, clicking on a link in an email or downloading something off the internet.

Data location

With so many people taking advantage of working from home or mobile working, there is the tendency for users to save business documents to desktops, personal devices or other inappropriate locations. The danger here, apart from data being unprotected on a personal computer or phone, is that the documents aren't backed up and therefore cannot be restored in the event of an issue.

Backup scope

In much the same way as users saving critical business documents in the wrong locations, many employees may save documents and folders on the company network in locations that aren't necessarily backed-up. As a result, users need to understand which areas of the server are actually backed up and which locations are best suited to save key documents and data.

Password policy

Passwords remain a bone of contention between cyber security teams and users in terms of their strength and changing them regularly. According to the Verizon 2016 Data Breach Investigations Report, "63% of confirmed data breaches leverage a weak, default, or stolen password". Weak passwords can easily be broken by malware, such as CryptoLocker, allowing hackers to propagate network resources and infect systems. This extends beyond user logon details and also applies to printers, phones and other network devices with passwords. As a result, the importance of proper passwords and password management shouldn't be overlooked.

Disaster recovery

Disaster recovery and business continuity plans are key to ensuring a company can function during a disruption – like a cyber attack – and effectively recover and carry on operating once it is over. While many businesses see the value in creating a plan, not many spend the time and money on testing them, which could affect their effectiveness when they are actually needed.

Infrastructure vulnerability

Due to myriad reasons, particularly budgetary ones, many companies still rely on legacy technology. The danger is that this out-of-date technology may not be supported anymore by vendors and security software, and may indeed be open to a range of security risks.

Conclusion

Successful cyber security requires a multi-layered approach and is constantly evolving to meet the needs of the business and address the changing threat landscape. A large part of this includes involvement and buy-in from the entire organisation, as well as a significant focus on mitigating the risk of human error through programmes such as user education. As cyber attacks grow in both sophistication and frequency, these steps have an increasingly important role to play in protecting the business and helping mitigate risk.

Link to the original article:
https://engageemployee.com/best-practices-making-cyber-security-work/