Cyber security: how can we turn the corner?

By Cliff Moyce - Tech Page One

Companies that manage data rely on customers being confident that their data (including personal details) will be held safe and secure. If this backbone of trust is broken, those using their systems will simply stop doing so. This applies at both a corporate and at a consumer level. The particular sensitivities and high level of personalisation and visibility that characterise many modern enterprises make privacy vital for businesses' continued existence.

Despite the importance of customer confidence in data security, there have been several high profile cyber security breaches in the past two years in which enormous amounts of sensitive data were stolen. Hundreds of other breaches have occurred in the same period, they just haven't made the headlines. Companies that have suffered loss of customer data include JP Morgan Chase, Talk Talk, Anthem, Ashley Madison, Patreon, and LastPass. Some of the problems suffered have been so severe as to threaten the future of the company.

In 2016 organisations will be keen to ensure they do not suffer the same problem, but how will they achieve that aim?

One important step for organisations wanting to reduce cyber-security risk will be to disavow themselves of the common misconception that data losses are usually the result of technology weaknesses, vulnerabilities and failures. In fact, it is human failings that are far and away the most common causal factor in what is usually reported by the press as 'hacking'.

Developing security policies to mitigate the people risk in cyber security is no longer enough. In fact it was never enough. Such policies risk being treated as a tick box exercise, or are created with good intent but are undermined by a culture of poor practice. Education and training in security policies is essential – but even that approach can fail if the necessary culture change does not happen.

This is where the most important change needs to happen in 2016 to avoid repeating the mistakes of 2014 and 2015.

All employees need to be trained and examined on cyber and data-security on best practice. One important area that is often overlooked is the risk of individuals falling victim to social engineering outside of work and that compromised status manifesting in their workplace. It is vital

that all staff understand how email attachments, phishing, and impersonations can be used to install malware devices to personal devices or work computers that can then obtain login credentials to a corporate network. At JP Morgan Chase it was an employee's personal computer that was infected. When that individual logged-in remotely to the corporate network via the company VPN in June 2014, the malware obtained access rights to the network. Further human errors (including forgetting to update software on one server) made it possible for the hackers to gain control of 90 servers and huge amounts of data.

If companies invest in the right training and education of their people, it will result in a renewed faith in data security, which would be a breath of fresh air for a world that is becoming increasingly wary of modern enterprise's ways of working (and understandably so).

One ray of hope is that many organisations are now establishing better security standards and looking for new ways to create more private and secure methods of communication and engagement. Hopefully the outcome will be that people will start to feel more confident in using the apps and services that have so much to offer in terms of personal productivity etc.

But will these improvements represent a triumph for everyone? Sadly no. The unfortunate loser of tighter security and greater awareness will be the advertising industry. For advertisers, new security standards will mean that they have to invest in, less intrusive forms of advertising. But hopefully that will eventually work for them as well as current methods, and any disruption will be temporary.

To finish on a cliché: every problem is also an opportunity. With knowledge will come greater online security, more educated users of technology, and (even) more sophisticated advertising!

Original article — http://www.techpageone.co.uk/technology-uk-en/cyber-security-can-turn-corner/