THE HUMAN FACTOR

Francois Rodriguez, *Chief Growth Officer at Adeya, looks at how the biggest threat to enterprise data security comes from within, and the steps needed to combat it.*

When it comes to data breaches, it is a case of when, not if, one will strike your organisation. No matter how much you've invested in your security, how bleeding edge the technology behind it is, a breach will happen, and critical, sensitive data could well be exposed.

Why? Most organisations set their security to deal with external threats. They acquire solutions that combat certain threats, whether malware, ransomware, denial-of-service, phishing, spear or any other type of cyberattack, and implement them. Just look at the traditional approach to protecting against digital threats, the firewall. It was designed specifically to keep threats out.

But this is not enough, and the reason is because most organisations consistently overlook the human factor. That is the impact employees can have, and how their actions, ways of working and attitudes compromise security. In fact, people are such a threat that, according to IBM research, 95 percent of all corporate security incidents involve human error.

And at a point when we have seen a massive change in the way businesses operate, and so many workers suddenly going remote, the potential for people-driven breaches is at an all-time high. Why? Because many employees find themselves in unfamiliar working patterns as bad actors look to exploit the chaos. But what do these human factors look like, and how can you protect against them without alienating employees?

95 percent of all corporate security incidents involve human error

What can be defined as human factors in data breaches? Simply put, it is any instance where the problem has been caused by human action, whether deliberately or by accident, rather than a fault in tech.

Some of the more common ones include:

Opening infected emails or clicking on attachments without considering the source of the email – this used to be primarily a consumer issue, but over the last few years it is being increasingly deployed against business settings. An email will purport to come from another business, particularly one the recipient already has a relationship with, with a message saying that further details of a request can be found in the attached PDF. By opening the attachment, the recipient runs the risk of allowing some form of malware to access their system. By doing so, attacks can bypass corporate firewalls by entering networks via email servers.

Social engineering and identity theft – linked to infected emails is the spectre of social engineering and identity theft. Particularly during the current pandemic, messages preying on the constant need for information and updates threaten to cause havoc as they prompt unwitting individuals to click on links if they want to find out about a miracle cure or a secret grant for businesses. More generally, there is the issue of identity theft. This used to be a drawn-out process which required criminals to gather data from different sources before opening credit cards and bank accounts in other people's names. However, scams have become more sophisticated – in a famous example, artificial intelligence was used to spoof the voice of a group CEO in a phone call with one of his country managers, resulting in the latter transferring almost a quarter of a million dollars to a third party's account. As well as highlighting the access that criminals have to the latest innovations, it also serves to demonstrate that every level of the business needs to be alert to the dangers of cyberattacks.

Shadow IT and the introduction of consumer-grade collaboration technology – while a common problem in enterprises where business need and IT control are often at odds, the threat of shadow IT, where unauthorised applications and tools are deployed outside of IT governance, was particularly prevalent during the COVID-19 pandemic. That is because, in the rush to keep employees safe while maintaining continuity, unprepared businesses resorted to deploying whatever technology they can acquire and use quickly to keep employees talking. As is becoming clear, particularly with the issues Zoom faced, the fact of the matter is that this usually means consumer-grade applications; popular tools and technology that do not have the levels of data protection and privacy that business requires. By continuing to use them, companies expose themselves to huge risks, not only through an increased chance of a breach, but from regulatory and compliance sanctions should they suffer an attack.

ACTIVITY OVER UNSECURE NETWORKS PROVIDES A HUGE OPPORTUNITY FOR DATA BREACHES

Connecting to free wi-fi or using untrusted GSM networks – while life in lockdown might temporarily preclude employees from using untrusted networks while on the move, it remains a major threat to enterprise security. Even while working from home, those suffering with poor broadband connection may be tempted to piggy-back on unsecure networks within range of their devices. The problem is that if they can, so can others, increasing the risk of exposure to bad actors. This makes it vital that enterprises equip workers with both the knowledge and the necessary tools (such as the ability to use a VPN while on an unknown network or public wi-fi), as any activity conducted over unsecured networks is a huge opportunity for data breaches to occur.

Avoiding these threats may seem straightforward, and more a matter of applying common sense than requiring specific policies and tools. Yet these are not ordinary times – employees are under immense pressure while still attempting to work through the current uncertainty. The speed at which everything has changed is unlikely to have left much opportunity

▶

for training, particularly in businesses less used to remote working. So simply assuming employees will understand what not to do is not enough. But what steps do enterprises need to take in order to limit the risk from their own workforce?

If businesses are finding that breaches are being caused by human behaviour, there is clearly an issue around culture, and particularly the company's attitude towards security. If employees (including senior executives) believe cybersecurity to be the responsibility of someone else, that needs to change.

The key principle is that every member of the organisation is equally responsible for security. If workers struggle to understand this, then education, training and communication needs to be implemented to make them realise that it is as much their responsibility as it is that of another department, whether that is IT or someone else.

It comes down to ensuring everyone understands what basic cyber hygiene is and how their individual actions are a critical part of it. Much of it is interlinked – knowing how emails can be used to get access to corporate networks will include education around not clicking on or downloading anything from unknown and unverified emails, but it also connects to a better understanding of social engineering scams. Miracle cures, too good to be true offers and 'secret' government news messages feed off current fears, concerns and insecurities, but if employees already understand what suspicious messages can look like, they will be less likely to fall for other ruses.

This in turn is linked to having a zero-trust attitude. By refusing to allow anything access to systems or information until it has been verified, whether application or device, employees will help ensure corporate data stays safer and networks are not compromised. Once they have that understanding, they will be more likely to realise why quick workarounds and easy-to-use consumer technologies can also be major security risks. It should also contribute to improving good behaviour around updating software – with less shadow IT, fewer applications will fall outside the boundaries of corporate IT governance. At the same time, employees will become more aware of the importance of keeping their own technology up to date, thereby closing another avenue to cyberattacks.

TRIED AND TRUSTED

There is also the importance of keeping data encrypted, both when it is at rest and on the move. Again, this is linked to using approved applications and devices, using trusted and secure communication channels and not sharing data unnecessarily.

These behaviours and ways of thinking are critical to ensuring that everyone, from executive to intern, is aware of their part and role in securing the company's critical data and networks. It needs to be built into the organisation as a whole, and it is one that has to be addressed now; as workforces settle into an indeterminate length of time spent in a decentralised way of working, they will quickly learn new behaviours and approaches to work. If these do not have security at their core, the impact on the business could be significant to say the least.

We are in chaotic times – exactly the opportunity bad actors look for to strike and ruthlessly exploit. To prevent this, organisations need to lock down all potential gaps in their defences as they adapt to their new realities. Deploying the right technology is important, but so too is ensuring that their employees understand their role and practice the appropriate behaviours. Workforces are faced with increased uncertainty; it is incumbent on employers that they do not overlook this human factor if they are to reduce the risk of breaches at a moment when they are already facing massive disruption ●

Francois Rodriguez – Chief Growth Officer, Adeya – is a digital business transformation leader with a track record in formulating and executing growth strategies global markets. He has over 20 years' marketing experience across industries.

Every member of the organisation is equally responsible for security