zivver

Insight

How to improve digital communication security across your organization

While digital transformation isn't a new phenomenon, over recent years businesses have been forced to escalate their digital strategies to thrive and, in some cases, to survive. Remote working, a rise in security incidents, evolving regulatory pressures; these are challenges faced across all industries today. Securing digital communications has never been more important.

Hybrid working has placed an enormous strain on IT resources and, in addition to shouldering the responsibilities of their day-to-day roles, employees are also positioned as data protectors, undertaking the burden of compliance.

But security is a complex subject. It's interesting to consider that those data breaches which are inbound threats (such as malware and phishing) seem to dominate the conversation, when, in reality, over 80% of reported data breaches this year were the result of human error (e.g. sending sensitive data to the wrong recipient, misuse of Bcc etc.). Therefore, expecting people to prevent every data incident is comparable to locking your front door but leaving the windows wide open.

With employees working away from the office, our reliance on sharing sensitive information online, in the moment, wherever you are, is increasing. Adopting a 'security culture' has become a buzz term for enterprises seeking to deploy a security-first mindset across remote teams. However, with data breaches on the rise, it is clear that compulsory training is failing us, and some of the tools employees use to handle sensitive digital assets are not fit for purpose.

But blaming people when technology or procedures fail builds a culture ripe for digital fatigue - something we are witnessing more today than ever before. Evidently, a traditional approach to digital communications security isn't working for most enterprises in today's digital world.

If it's broken, fix it: How are early generations of digital security failing us?

With the widespread adoption of hybrid working, the explosion of data, and the roll out of data protection regulations, the first generation of digital security lacks all of the functionality required to ensure compliance today.

For example, often it is the case that traditional solutions have an inadequate email revoke function; they lack multi-factor authentication to verify a recipient's identity, and people have zero control over access once an email hits the recipient's inbox, or whilst the email is in transit. We also see that some vendors retain access to decryption keys, meaning email data is not protected or safe.

Employees are cornered daily by obstacles dressed up as security functionality. Instead of adopting security best-practice, busy employees are becoming experts in how to navigate obstacles inbuilt into workflows, jumping outside into different environments such as third party file sharing platforms and unencrypted messaging applications.

Simply put, earlier generations of digital security platforms are coming up short of what is required today.

Third generation: The real value of digital communications security

With the hyper acceleration of digital transformation, regulatory reforms and hybrid work, we all need a modern secure communications platform that is highly usable, empowering secure work with maximum effectiveness and minimal disruption.

It's ironic that we have smart cars, smart homes, yet smart digital security solutions to protect the most sensitive of assets, until now, haven't existed. Innovative new solutions go above and beyond adopting a security culture, enabling enterprises to affect an instinctive security lifestyle, wherever their employees are based.

In essence, the 3rd Generation of Secure Digital Communications is:

Effortless – the ability to operate within existing email tools intuitively and with a high ease of use – think 'one click'

Secure – not just 'good enough' but has a high level of end-to-end data protection, with zero keys, zero access, unparalleled encryption and user authentication

Smart – semantic aware with tailored levels of data protection, along with machine-learning driven business rule-based error correction

Earlier generations of technology are not up to standard. They do not keep pace in today's world and cause friction in everyday workflows. It's time for a new generation of effortless, smart and secure digital communications.

zivver

Ready for a deeper dive? So are we.

Request a free demo