FUJITSU

Why hybrid working does not have to compromise cybersecurity

Written by Financial Times

November 2021

Strict security measures can undermine the seamlessness of remote working. But with hybrid working here to stay, can organizations find a way to ensure the security of all company data and systems while empowering employees to do their jobs remotely?

Why hybrid working does not have to compromise cybersecurity

The future of the workplace looks set to be a hybrid one, but are organizations prepared for that future? That depends on their cybersecurity.

As organizations adopted new ways of working, cyber attacks became more frequent and increasingly inventive. Remote work has caused the average cost of a breach to increase by $137,000.

Now, organizations are seeking to establish hybrid working as standard. Fujitsu research, for instance, finds that 49 percent of global firms have adopted hybrid working in a bid to boost the agility of their workforce. This means that more employees will be accessing critical and sensitive data and systems from different devices and locations. Restricting access to these systems would hinder the agility of remote working, but unimpeded access would make company data vulnerable to cyber attacks.

How do organizations adapt their security to this new way of working while protecting company data?

Changing risks need a new attitude to security

The cybersecurity needs of employees will continually evolve as hybrid working allows them to “pick up the closest device or the one that is most convenient”, according to Christian Reilly, VP, technology strategy at US software firm Citrix.

“They want to access what it is they need to be productive at that moment in time, instead of sitting at a desk in front of a giant screen,” he says. “That poses a huge challenge in terms of security, policy and operationally, and from an HR and future-work perspective, too.”

The Fujitsu research reveals that fewer than six in 10 organizations are aligning their cybersecurity approach to employees’ needs in this rapidly changing work environment. Part of the reason for this is that cybersecurity teams can be too cautious and inflexible, according to Laura Whitt-Winyard, head of global information security DLL Group, a vendor finance company.

“The first impression of security was always the ‘no’ group,” she says. “The group that makes developers' lives crazy, the group that is a cost center and not a value-add. We need to change that script.”

Whitt-Winyard adds that convenience does not have to be the nemesis of security — it just needs an attitude shift. “I am challenging my team to realize that every single person at DLL is one of our customers, and it is our job to help them to partner with the business and understand why we do security and sometimes even how we do it,” she explains.

There is a security/experience compromise

Citrix's Reilly says that organizations have to strike a balance. "Security is extremely important, but too much security leads to a bad user experience and too much user experience usually leads to bad security," he says. "We have addressed that challenge by focusing on somewhere in the middle."

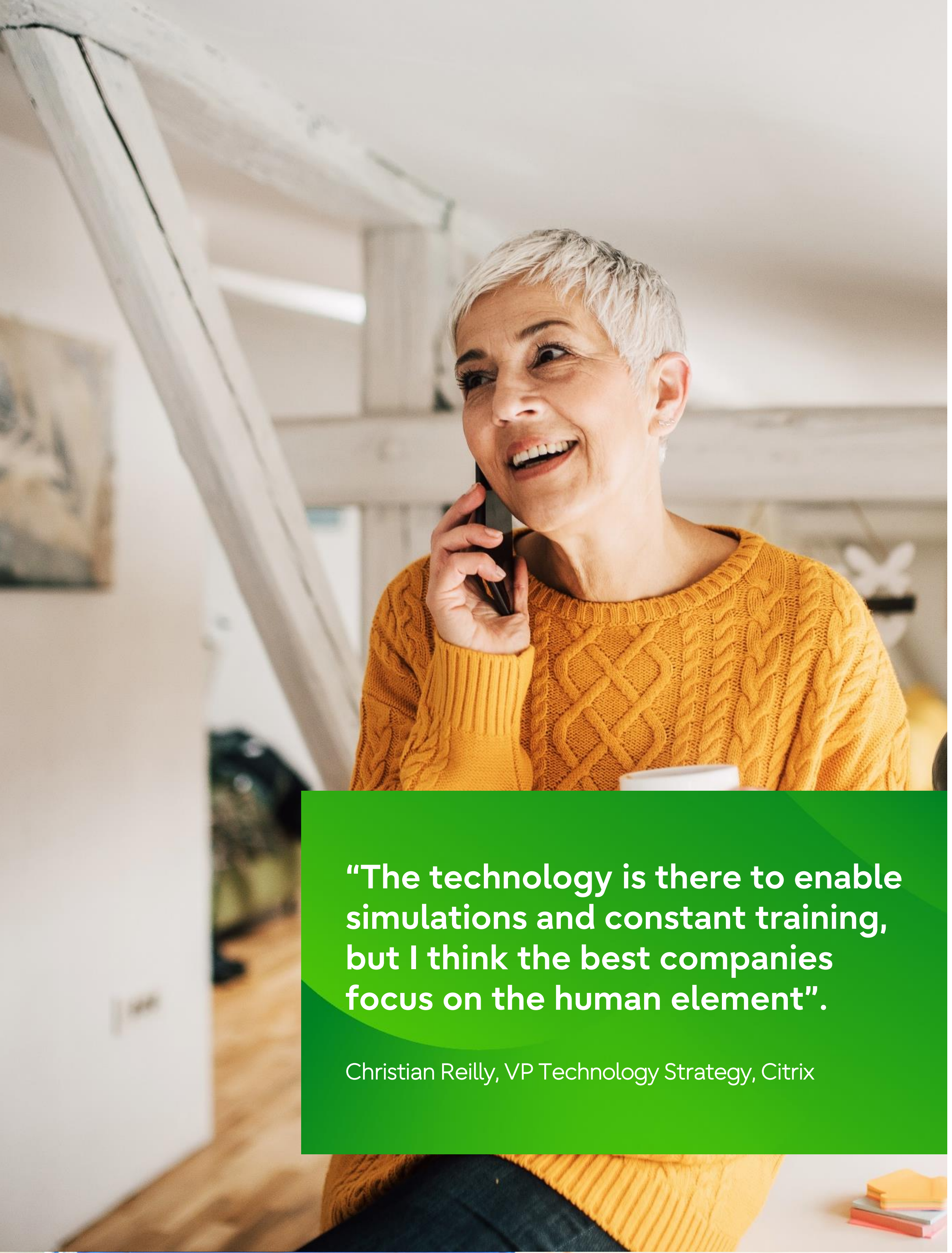
Greater engagement between technical and non-technical employees can be one way to find this balance. Research carried out by Fujitsu in 2020 found that there is a significant misalignment in the views of "technical employees" working in cybersecurity, software and technology and "non-technical employees" working in other departments, and this can lead to a breakdown in communication.

So, organizations should encourage clearer dialogue between employees and the IT teams in charge of cybersecurity, and the latter group seems to recognise this: 73 percent of technical employees expect collaboration between cybersecurity and other departments to increase.
This is what it all is about, we need to focus on this balance between the user experience and security.

73 percent

of technical employees expect collaboration between cybersecurity and other departments to increase.

Fujitsu Research Study: Building a Cyber Smart Culture



Humans are the weakest link

Reilly says that cybersecurity teams will have to work to understand the “human element” of cybersecurity. Technology is crucial to ensure technical competence against threats, but organizations also need their employees to have a grasp of why cybersecurity matters.

“The technology is there to enable simulations and constant training, but I think the best companies focus on the human element,” he says. “Because ultimately the human is the weakest link in the chain.”

Communication can help to strengthen that link. “We have increased a lot of our communication,” says Whitt-Winyard. “We created a group chat so that anyone at DLL who has any questions about cybersecurity can reach out to us and get real-time answers.”

However, Fujitsu’s research shows that only 52 percent of businesses are communicating regularly with their teams about the importance of working safely online. This lack of communication may rest on the belief that employees already understand the risks: 68 percent of respondents say that all employees in their organization understand the security risks they face and their responsibility to protect the organization when working remotely.

But organizations should not be complacent. Research by Chatham House, for instance, finds that the Covid-19 pandemic has “only served to provide perpetrators with new opportunities and vulnerabilities to exploit”.

> **“The technology is there to enable simulations and constant training, but I think the best companies focus on the human element”.**
>
> Christian Reilly, VP Technology Strategy, Citrix

Invest strategically in training, trust and technology

Organizations need to invest in regular cybersecurity training: only 43 percent of Fujitsu's respondents say their organization provides ongoing cybersecurity training for employees. Reilly says that some of this training could take the form of "simulated phishing attempts", whereby employees are given a safe environment in which to identify efforts to install malware.

More advanced security measures include data leakage protection and digital rights management protection, and behavioural analytics services that identify unusual behaviour. In the Fujitsu research, these are already implemented by 36 percent and 23 percent of firms respectively.

Then there are solutions that are especially appropriate for hybrid working, such as zero-trust systems. This approach to the design and implementation of cybersecurity systems assumes that individuals should not be able to access company systems until they can prove their trustworthiness. A 2020 study by IT service management company Okta found that just 40 percent of firms globally are working on zero-trust projects.

Innovative technologies such as artificial intelligence (AI) and machine learning (ML), meanwhile, can also play a role in cybersecurity. Whitt-Winyard says that DLL has AI and ML tools that detect anomalies in user behaviour and is planning to increase its use of these technologies in the next 12 months.

By training employees to work in a cybersecure way and enhancing security with advanced measures, organizations will achieve two things: effective protection for their data, and a seamless remote working experience for their employees.

This content was paid for by Fujitsu and produced in partnership with the Financial Times Commercial department.