How to reimagine security and stop holding back employee productivity

By Ichiro Ohama,
Fujitsu Senior VP, Enterprise Cyber-Security

Spare a moment for the people in your organization tasked with ensuring cyber security. Put your gripes – and I know you'll have some – to one side for a moment.

Every day, the gatekeepers of systems and data have the uncomfortable task of balancing productivity and ease-of-use with security requirements that work. How exactly do you prioritize security without burdening employees with endless processes, documents and passwords?

It's not quite as reductionist as this, but if users find security measures restrict their productivity too much, they're going to try to bypass or overcome them. This does not improve risk and vulnerability.

If the task of balancing these contradictory needs is delicate, it also has to be carried out in a moving landscape. Cyber threats are continually changing, and new threats are emerging. One striking example is the COVID-19 pandemic.

Many employees had to leave the corporate network's safe confines and use potentially less secure home devices and networks to access corporate systems and data.

Attackers exploited this trend, focusing on themes that would look relevant under the new circumstances. There were vast quantities of phishing emails promising exclusive information about COVID-19; bogus web sites to trick users into typing in usernames, passwords and banking details for donations; and fake relief efforts or temporary government loans and grants. And not every organization was able to deploy the right infrastructure with the proper security measures from the start.

Making IT more secure comes at a price

But let's not be too forgiving. We can probably agree that the way users experience security can be frustrating and cyber security specialists indeed have to shoulder some responsibility. Many things users want – need – to do during the day make cybersecurity specialists feel insecure. Like using personal devices without updated anti-virus software, or unchecked USB sticks with the potential to infect entire corporate infrastructures.

That's why organizations develop policies that ban these things. The intention is to make things difficult for cyber criminals – but with the side effect of sometimes hampering employee productivity. But people have to work and that almost inevitably leads to an 'exceptions' policy. After a few weeks, everyone has applied for an exception, leaving the original system in tatters.

As well as putting users through laborious processes to use IT, cybersecurity can also be about preventing access to IT in the first place, for example, blocking the use of potentially valuable cloud resources. What's that all about? Alongside the agile upside of so-called 'shadow IT', there is an anti-resilient downside. Business departments have sourced cloud services without considering cyber security and IT infrastructure holistically. Why should they? It's not their responsibility. But when it comes to things like data protection and privacy and tasks like data replication and backup, not applying the corporate rules can lead to a host of complications – some of them very severe indeed.

What makes everything even worse is that users regularly get to experience more advanced or more convenient security measures in their personal lives. We have all sampled the simplicity of fingerprint or facial recognition to unlock a phone – and find this much more convenient than a corporate policy requiring a password change every 90 days.

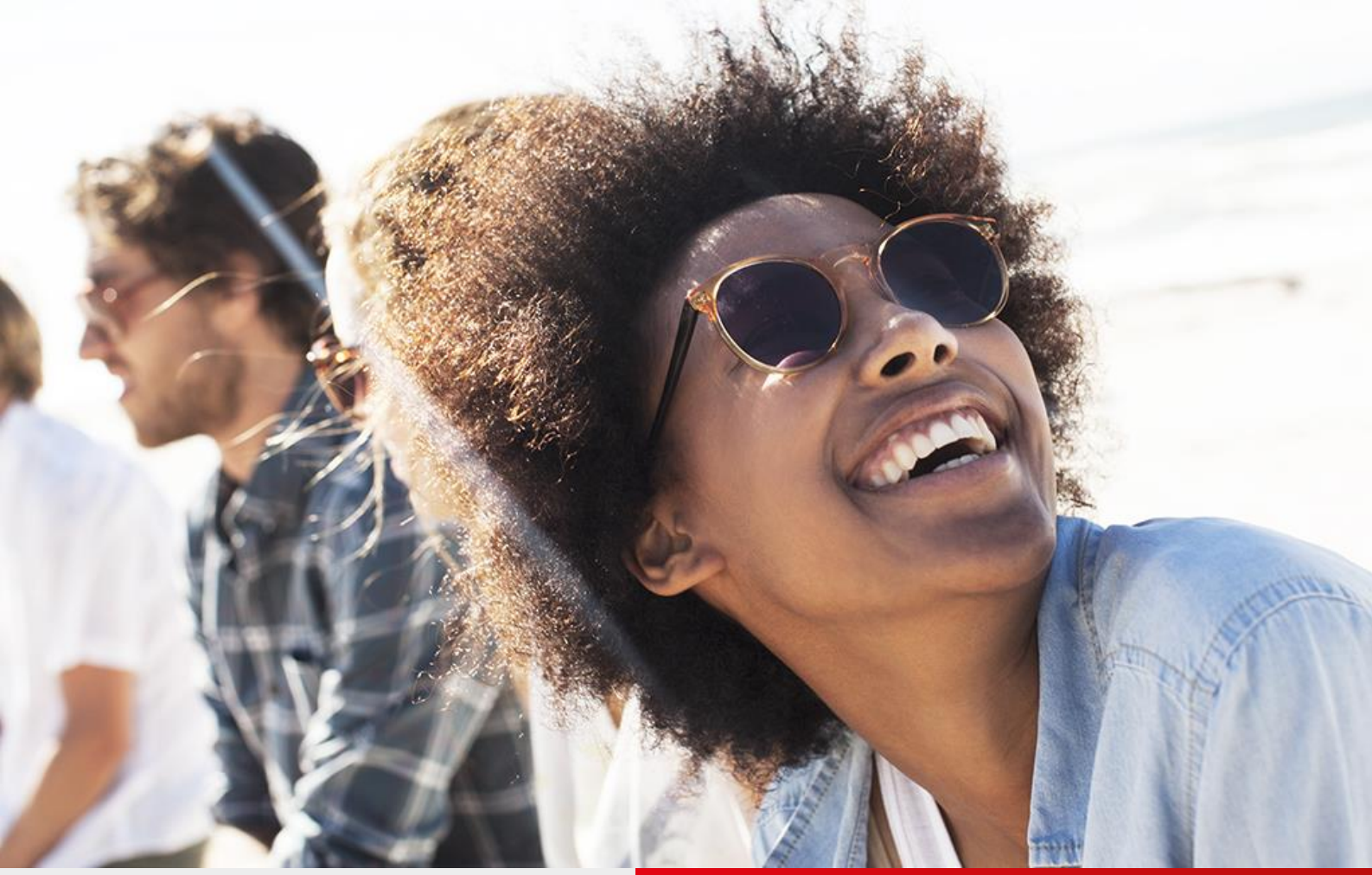
A better way?

There has to be a better way. We need to create a consumer-grade experience with a corporate wrapper as secure as we can make it. These are almost diametrically opposite needs, with a tension complicated to resolve: it is a challenge to create a better user experience while deploying security measures for organizations working across various countries and partner organizations. And simple economics dictates that any new system will be in place for quite some time – meaning that it is always likely to look dated against the latest consumer tech.

One thing we can agree: Where we are today is no longer fit for purpose. IT departments create long policy documents and force employees to review them annually, but the do's and don'ts must translate into something more dynamic. It's a massive change, but the necessary changes are starting to come through.

What this points to is that the people aspects of security are often more complicated than the technical. And ironically, new technologies could make things even more frustrating for users. What's needed is a corresponding change in security culture that treats users more like consumers, so we get away from the once-a-year security training event to something more interesting, enticing and lasting.

Getting there will require business and security teams working together, understanding and agreeing what risks are unavoidable (and planning appropriate security measures) and those where the risk outweighs any likely potential reward. Security has to speak the language of business.



Understanding the security context

As a starting point, cyber security needs to have a better handle on users. Today, access rights are generated service by service or system by system. This approach is too crude and too complicated. There are fewer face-to-face meetings now, but the need for executives to access corporate systems remotely remains. Blanket bans are unworkable and unnecessary.

Security is now moving towards persona-based rules, mapping reasonable behavior for that person, and applying it dynamically. This is already in place in many organizations – at least in a rudimentary way. What's likely to be missing is context-sensitive role profiles, dynamically created for different types of users accessing data outside core working hours.

New 'digital experience' roles assist the shift in enterprise IT, modeled on the consumer environment, where services and products have experience 'champions' to ensure what is delivered is actually what the user wants and needs. For the enterprise user, this isn't just about making it look good: the task is to protect value streams delivered by how people work and to add value by mapping end-to-end workflows. The way forward is for cyber security and the enterprise experience owners to build in the right security as part of the design.

Towards a new security culture

The new way: emulate the launch of a consumer product. Look at the total experience for the 'customer' and design-in security as part of the overall value workflow. If we have the digital experience owner, we have a starting point to add value to the people who generate value.

But users have a role too. Security teams can work as hard as possible to make everything' secure by design.' Still, unless users take responsibility for doing their part, no amount of smart technology will keep an organization entirely safe. When reimaging how every employee can contribute to an organization's security posture and building a culture that fully integrates intuitive security, everyone plays a crucial role.

Learn more about how we can help you reimagine your everyday operations and get in contact with one of our technology experts.