IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

In Conversation

In Conversation with John Gilbert

Carol Baker

According to the authentication and security experts at Yubico (https://www.yubico.com) more than three quarters of enterprises in the UK, France and Germany have yet to see the value in implementing two-factor authentication. With research exposing poor password hygiene – as 54% of all employees reuse passwords across multiple work accounts, and over 40% of business owners still remember passwords by writing them down – we talk to John Gilbert, Regional Vice President at Yubico for his views on the research findings.

***John Gilbert** is Regional Vice President at Yubico (https://www.yubico.com).*

With more than 25 years' experience in the industry, John is a tech industry veteran who specializes in security and identity assurance.

Day-to-day, he works closely with Yubico's existing and prospective customers, supporting them in embracing stronger authentication as the cyber threat landscape continues to evolve.

John is also an authority on open authentication standards, including FIDO U2F and FIDO2.

Tell us a bit about Yubico

Yubico is now becoming a household name within the authentication and security market.

The company was formed some 13 years ago by a husband and wife team in Stockholm, Sweden. Their ambition was to make the internet a safer place for everyone. If you look back to that period, it was the birth of the kind of identity theft which we are now familiar with on the internet. They wanted to secure identities both for individuals and businesses. That was really the foundation and the founding ethos behind Yubico – and it continues to influence everything that we do today in terms of our development and in the way the company operates.

Over the last six to seven years, we have grown very rapidly and our YubiKey technology has become the trusted secure authentication choice of some of the largest technology, finance, manufacturing and retail companies in the world. That


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

growth has been founded on a twin track approach to innovation, where we've been involved heavily in redefining, building and driving the adoption of new standards for user authentication, and in driving new security standards in terms of verifying and identifying individuals.

We have played a key role in establishing those global open standards through the FIDO Alliance – a collection of organizations large and small, across the globe, all of whom share an interest in progressing open standards-based authentication. The FIDO Alliance has grown significantly over the last four or five years with everyone from very large banks and insurance companies, to manufacturing organizations and so on, all participating in the Consortium.

Being a founding member of FIDO, Yubico was heavily involved in producing a standard named Universal 2nd Factor with Google. FIDO U2F is a standard that Google still uses today to secure its networks in conjunction with hardware-backed security keys. Indeed, Google has expanded its deployment of the YubiKey to all staff and contractors for secure computer and server login, reaching more than 50,000 employees.

As a result, Google has benefitted from heightened security, with internal accounts protected solely with a YubiKey and FIDO U2F, as well accelerated employee productivity and reduced support. The technology behind the YubiKey has accelerated and changed over the last five years, as we continue to evolve to incorporate new standards and make our offering more relevant to companies and individuals.

Building on that experience, our work with Microsoft has brought us to the attention of a much wider audience with the development of FIDO2 – a standard which is now built into the Windows 10 operating system and forms the core of Microsoft's cloud-based authentication strategy moving forward. This means Microsoft Azure, Active Directory components, and Microsoft's own tools as well as third party products, all rely on the FIDO2 authentication standard.

Tell us more about your research findings

Our research[1] into the 'Cybersecurity in the work from anywhere era' surveyed over 3,000 companies across Europe, including the UK, Germany and France. Some of the findings were very interesting, but perhaps not surprising to us.

Poor cyber hygiene is nothing new. However, the sudden and widespread shift to remote work has thrown many cybersecurity practices up in the air. We have seen a complete role reversal, if you like – users who are used to being ensconced in offices, with firewalls around them and corporate IT teams on hand, suddenly found themselves working in their own homes with all the distractions that this brings. And that's a very difficult work adjustment.

Of course, there has always been a percentage of the workforce working from home, but now we are seeing that shift to the majority of the modern workforce, which presents some real challenges. We've seen the corporate security perimeter


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

being pushed out to people's local IP addresses and their home routers – and very often, we know that those kinds of devices are less well protected than they would have been if they were within a corporate environment.

For example, on my broadband router I happen to have a very strong password, but there are many people who simply use the same password that came with the router (often it is something like admin123), and almost all bad actors will be able to figure that one out.

So, if you are someone looking for ways into an organization, especially one with people working from home, you are going to look at weak points in that infrastructure to exploit.

Likewise, when your users are working in the office, they are protected by the IT department to a certain extent and do not have to think too hard about data protection and phishing attacks. At home, amongst familiar surroundings – perhaps working from the kitchen table, with pets and/or children running around, or someone at the door – they are more likely to make a mistake in a moment of distraction, and it becomes easier for security to be breached.

Do you think IT departments are ready to handle the hybrid workforce?

When staff begin returning to the workplace, some bad habits are likely to return with them – and that is creating concern.

IT departments will need to update their security strategies to cater for the hybrid workforce. We are seeing more companies embrace cloud-based security options, moving from on-premise to cloud. This gives organizations the opportunity to take advantage of certain Modern Authentication standards such as FIDO2, and the use of security keys.

By embracing cloud and with the greater use of single sign-on (SSO) technology it makes user experiences smoother from the point of login to their individual device, all the way through to accessing the assets within the business which they are permitted to see. This plays out very well across both on-premise and when working from home.

Are employees becoming more, or less, confident in spotting phishing attacks?

Our research found that there's a degree of overconfidence in spotting phishing attempts. Whilst there's been a fair bit of press around phishing, I'm not sure it always hits home for your average user that these attacks are often highly targeted, and even less sophisticated attempts can catch people out in a moment of distraction.

This perceived overconfidence revealed quite a variance between the types of employee and the industry sector they are working in. For instance, savvy users who interact with technology daily, may suffer from a degree of overconfidence. In


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

contrast, workers not used to interacting with those environments regularly – such as frontline workers in healthcare and manufacturing, for example – are just as vulnerable as anyone else to phishing. Despite this, they're probably less capable of actually spotting a phishing attack. In any case, it is important to remember that with the right combination of factors, almost any of us can be caught out.

It was interesting to see the results based on job role. Business owners often put their heart and soul into growing their businesses, and may have trained themselves to spot a scam from 1,000 miles away. A lot of senior execs and business owners live their lives through their laptops and portable devices – and they often don't want to keep switching between devices for work and personal matters. As such, they sometimes tend to mix the two and our research points to the dangers of doing so.

Good cyber practices and cyber security hygiene needs to come from the top down, and business leaders should lead by example. The challenge facing the IT department is to make that a secure, but simple process. This means any additional steps the user needs to take risks them trying to circumvent the requirement. Users want a combination of convenience, simplicity and a high level of security. This is the push-pull challenge that security teams live with everyday, and is exactly why we believe superior forms of authentication are required to enhance both security and the user experience. Particularly hardware-based authentication.

What about the role of 2FA and MFA in security solutions?

The role of 2FA and MFA is paramount within an organization. It's interesting when you consider the industry research that's out there. If you look at recent findings from Verizon[2], more than 80% of data loss, data breach and data theft can be consistently traced back to stolen credentials – it's usually the way that bad actors find their way into an organization.

Today, we see companies spending a lot of time and money focusing on the 20% that isn't related to stolen credentials, such as making sure firewalls are in place. In reality, 80% of the problems could be addressed simply by implementing a good level of authentication. 2FA and MFA is essential in my opinion, for any organization that wants to guard against data theft and breaches.

What are some of the pitfalls companies need to avoid when rolling out a passwordless strategy across the organization?

There is often a misconception that passwordless is a destination. Instead, it should be thought of as a journey – a journey that some organizations are a bit further down the road with than others. It also means different things to different people. Passwordless has been around in one form or another for a very long time. If you go back to traditional Public Key Infrastructure (PKI) authentication and the use of certificates, then you know this eradicates the password, and that's been part of Microsoft's on-premise technology for a long time. The challenge with some

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

of those technologies is that they've been difficult to manage. They are often cumbersome, involve a lot of time and effort, and they're quite expensive.

Organizations should recognize all possibilities of the journey. They need to think about where they want that passwordless experience to start – and my advice would be to look at implementing that at the point of first contact. If you can create strong, secure user authentication without the need for a password on the device, the domain or the corporate network, then hopefully they are in a strong position to flow this authentication of credentials through all other applications. By using technologies like SSO you can ensure that the secure credentials are passed on to any additional applications the user is allowed to access.

Combine this with conditional access policies and other methods of securing users, and you are well on the journey. However, this is not something you can simply press a button to resolve tomorrow. A lot of organizations live with legacy technologies that aren't passwordless-friendly, so they need a strategy to establish how to evolve that infrastructure. That's where the Yubico and YubiKey come in.

Closing remarks

A key takeaway of the report is the need for organizations to begin this journey that I talked about. Take a good look at your current security, how you protect the user accounts of your employees (and those user identities) and start to explore whether you can implement strong multi factor authentication in one form or another. Consider whether you are able to accelerate the adoption of modern authentication standards such as FIDO. If not, then look at what the other alternatives are, and make the choice to take a step forward. Now is the time to do it.

Also, be sure to invest in training – as our report shows that there's still a significant gap here. Many users don't feel supported, or even understand what they need to be looking out for when it comes to phishing attacks. There are some very smart training packages out there to help spot such attacks, so start building that user awareness and make security part of the DNA of the company.

Reference

[1] Yubico, *Cybersecurity in the Work From Anywhere Era – Findings on Employee Attitudes and Adaptability to At-Home Corporate Security*. Available at https://pages.yubico.com/cybersecurity-in-the-work-from-home-era.html

[2] Bassett, G., Hylender,C., Langlois, P., Pinto, A., Widup, S., *2021 Data Breach Investigations Report – Reduce risks with insights from more than 5,250 confirmed breaches*, Verizon. Available at: https://www.verizon.com/business/resources/reports/dbir/