Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company’s public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.
information that they were not allowed to access, either by working without it or asking the customer for permission to access it. How does this work? By tagging each piece of customer data with metadata – effectively creating a granular permissions system.

From the Data Protection Officer’s (DPO’s) point of view, the learning curve lies in grasping how to effectively write policies that can be implemented at the server level, but the advantage is that you don’t have to trust the app team not to request data that they aren’t allowed to see – you can enforce policy without having to have a detailed view of the inner workings of every app in your ecosystem.

It is a paradigm shift that fundamentally changes the relationship between the CDO and the development teams. Rather than trying to micromanage the individual teams – and even the relationships between them – it becomes a one-to-one, top-level negotiation centred on principles rather than fine-tooth code reviews. It delivers a high level of assurance that data privacy protocols are being observed consistently across the web services environment and beyond – and even opens the door to the next level of relationship with your customers.

Taking it to the next level

Once you have confidence in your data policy enforcement, it opens the door to explore a new, more personal relationship with customers and their data. Personalisation allows you to deliver an enhanced customer experience so that those who are interacting with the customer – whether that be an app or a human customer service representative – can deliver a consistent experience safe in the knowledge that they are working with a consistent and appropriate data package for that customer.

For instance, if a bank customer enquires about a service online and then goes into the bank a couple of days later to discuss something else, bank staff could remind her about that inquiry, provide more information and perhaps even close a sale. Or customers who browse an online retailer might then start using the store’s mobile app and you’d want to be able to track them across and say, you know those items you were looking at a few days ago? – they’re on sale now.

While it might seem like a simple thing to store customer preferences, in reality there’s a lot going on behind the scenes – specifically with identity – that makes that very difficult. Despite the obvious value to enterprises of using this technique, surprisingly few companies are doing it – and that’s because it’s actually not as easy as it looks to create a unified customer profile across multiple applications.

About the author

Dustin Maxey is a product and solution leader at Ping Identity (www.pingidentity.com) in the customer identity and access management (CIAM) software space. Domain expertise in enterprise security, hands-on engineering experience, raising venture capital, and founding several start-ups have given him a unique perspective on the critical elements of customer identity as well as the value that customer identity can provide to businesses.

Resource

- Teixeira, Henrique; Kelley, Michael; Allan, Ant; Care, Jonathan. ‘Gartner Report: Technology Insight for Customer Identity and Access Management’. Gartner, 4 May 2020. Accessed Aug 2020. www.pingidentity.com/en/resources/client-library/analyst-reports/3506-gartner-ciam-technology-insight.html.
only around 1.7 million people worked mainly from home, while 8.7 million (less than 30% of the total employed) ever worked from home at all.\(^1\)

For many of the millions who have recently made the adjustment to full-time remote work, it has been a whole new experience. Even so, it’s a change that is likely to stick for many firms, at least for a higher proportion of the workforce than ever before.

A number of studies suggest that the homeworking trend in the UK will continue. O2/ICM research, for example, found that 45% of workers predict permanent changes to flexible working when normal conditions resume.\(^2\) Meanwhile, Global Workplace Analytics in the US estimates that 25 to 30% of the workforce will work from home multiple days a week by the end of next year.\(^3\)

### Decentralisation of security

For both employers and employees, homeworking comes with pros and cons. For employees, it may confer a range of lifestyle benefits and completely eliminate the cost of the daily commute. These upsides weigh against the disadvantage of no in-person team working, which many people are used to from being in the office. Employers, meanwhile, may welcome the reduced need for expensive office floorspace and employees no longer clocking in late due to travel issues, but may rue the loss of creativity that can come from reduced collaboration.

Having said that, the great strides that have been made in collaboration tools and remote access, along with the increasing sophistication of devices, have facilitated the ability for employees to work remotely at scale. Yet, alongside the benefits of a dispersed workforce come some downsides.

Among those might be the decentralisation of security practices. Security practitioners will already have felt the pressure of supporting a workforce that had to transition to remote working suddenly. Employees must be equipped with appropriate security tools and the knowledge of why it is important that they are used correctly, to ensure the security of company data and the protection of assets.

The rapid development of Covid-19 will have left many organisations without the time or resources to install extra security on work-issued devices. For some, there may not even have been the budget or capacity to issue corporate devices at all. All of this means that many employees are working on less secure devices while at home, and on less secure networks than

---

**Levels of homeworking in the UK in 2019. Source: Office for National Statistics.**

- **Extraterritorial organisations**: 19.8% (Ever work at home), 18.6% (Work at home in the week prior to interview), 33.3% (Mainly work - own home)
- **Households as employers**: 14.3% (Ever work at home), 10.8% (Mainly work - own home)
- **Other service activities**: 30.3% (Ever work at home), 16.8% (Mainly work - own home)
- **Arts entertainment and recreation**: 20.3% (Ever work at home), 17.4% (Mainly work - own home)
- **Health and social work**: 20.3% (Ever work at home), 17.4% (Mainly work - own home)
- **Education**: 53.3% (Ever work at home), 46.3% (Mainly work - own home)
- **Public admin and defence**: 33.3% (Ever work at home), 29.4% (Mainly work - own home)
- **Admin and support services**: 33.3% (Ever work at home), 23.2% (Mainly work - own home)
- **Prof scientific technical activities**: 40.3% (Ever work at home), 26.3% (Mainly work - own home)
- **Real estate activities**: 38.5% (Ever work at home), 22.8% (Mainly work - own home)
- **Financial and insurance activities**: 32.8% (Ever work at home), 14.8% (Mainly work - own home)
- **Information and communication**: 32.8% (Ever work at home), 14.8% (Mainly work - own home)
- **Accommodation and food services**: 10.0% (Ever work at home), 6.5% (Mainly work - own home)
- **Transport and storage**: 13.4% (Ever work at home), 6.2% (Mainly work - own home)
- **Wholesale repair of vehicles**: 25.9% (Ever work at home), 10.2% (Mainly work - own home)
- **Construction**: 20.4% (Ever work at home), 6.5% (Mainly work - own home)
- **Water supply sewage waste**: 1.9% (Ever work at home), 1.9% (Mainly work - own home)
- **Electricity gas air cond supply**: 29.6% (Ever work at home), 13.6% (Mainly work - own home)
- **Manufacturing**: 21.1% (Ever work at home), 9.3% (Mainly work - own home)
- **Mining and quarrying**: 24.8% (Ever work at home), 8.5% (Mainly work - own home)
- **Agriculture forestry and fishing**: 39.0% (Ever work at home), 13.7% (Mainly work - own home)
usual. This will only heighten the pressure already felt by companies to mitigate security risks and shore up defences across all devices and applications.

Unfortunately, opportunistic cyber criminal are exploiting the uncertainty and vulnerability of these times and targeted coronavirus-themed phishing attacks have been seen.\(^4\) It is an issue highlighted by the National Cyber Security Centre (NCSC) in a joint UK/US security advisory.\(^5\) The communication covers specifically the exploitation of home working infrastructure and software as well as ways in which Covid-19-related scams and phishing emails are targeting individuals and businesses.

**Sophisticated threats**

The increased risk of phishing attacks – through which employees may be tricked into providing information such as login credentials – coupled with decreased employee security heightens the need for strong authentication and robust security practices.

Unfortunately, too many organisations still depend solely on passwords to gain access to devices, applications and networks. Yet, passwords come with a range of inherent weaknesses – they can be easy to guess, they get reused and, of course, they can be phished. Credential stuffing attacks depend on the ill-advised practice of password reuse.

Despite the risk, such behaviour is incredibly common. Recent Ponemon Institute research of UK IT professionals and employees found that 39% of individuals reuse passwords across workplace accounts and, even more worryingly, 51% sometimes or frequently share passwords with colleagues.\(^6\)

Strengthened authentication practices should focus on usability, as adoption of new technologies and approaches will be enhanced if they are convenient and easy to use. Whether employees work from home or not, they need a simple and safe way to create, store and manage passwords, and hardware security keys integrated with enterprise-grade password managers can help deliver this.

**The key to authentication**

Multi-factor authentication (MFA) provides a valuable additional layer of security for business IT networks. What’s more, in an environment where employees are routinely using home networks – which are often less secure than business ones – MFA provides reassurance that access to corporate applications and systems is robustly protected.

While two-factor authentication (2FA) – through memorable words or SMS one-time passwords (OTPs) – will be familiar to many users from services they access in their personal lives, it too can be susceptible to phishing, as well as man-in-the-middle (MitM) attacks. SIM-swap fraud is also becoming increasingly common.

Basic software-based MFA that texts or emails a code is a step up from simple log-in/username, but it isn’t without its drawbacks. From a user perspective, inputting answers and passcodes can be error-prone and adds time to the process of getting logged in. Users tire of lengthy, inconvenient stages in authentication that reduce productivity by putting up barriers to work getting done.

Hardware-based MFA tools, such as security keys, provide an alternative way to boost authentication security by proving that the person accessing the device or application is who they say they are. They also come with the added benefit of being simple and convenient to use.

Security keys can also help address the oft-neglected issue of mobile phone security, which is also heightened at these times of remote working. Despite many employees routinely accessing applications for work purposes from their phones, 55% of UK organisations responding to the Ponemon survey said they didn’t believe necessary steps had been taken to protect information on mobile phones. This gap in security should be closed to prevent potentially damaging breaches.

**Extra protection**

Additional approaches to protecting company data handled by employees working remotely include end-to-end encryption and VPNs. Encryption can be used in conjunction with a VPN or on its own but is usually limited to a particular service or application.

A VPN will protect data from device to server, but beyond that, it is exposed to the Internet. To provide an extra layer
of security, it is possible for some VPNs to be configured to work with a security key for remote access.

Cloud environments support the drive towards remote working without compromising on collaboration. Identity and access management (IAM) solutions ensure that companies know who is viewing what, when and why, as well as provide an overview of network usage. For employees working remotely, single sign-on is convenient but should those access credentials become compromised, it can potentially open up access to multiple applications and information sources. Here again, MFA helps mitigate the risk of data falling into the wrong hands and of cyber attackers getting access to a range of services.

Making it work for workers

As employees adapt to unfamiliar work environments away from the office, their primary focus is not necessarily on security and robust methods of authentication. For the security practitioner, the sudden and far-reaching change in working practices, together with employees who are spread out geographically and potentially using a range of non-standard devices, presents a challenge to the maintenance of strong and secure cyber security.

It is important that any potential security gaps created by the change in working practices are plugged to prevent company data and assets from becoming at risk. Increasing authentication protocols to go beyond username/password combination, with the inherent weaknesses therein, will help shore up defences against a range of cyber threats.

Superior methods of MFA, such as a mobile authentication app or a hardware security key, boost security without unduly inconveniencing users. This is important because employees will feel more cut off than usual from IT support at this time of remote working and need to feel confident in the equipment and processes they’re required to work with. Authentication protocols need to work well for employees, while providing the right level of protection for networks, systems and data.

About the author

Nic Sarginson is senior solutions engineer for UKI and RSA at Yubico (www.yubico.com). An industry veteran, he has held a range of roles within networks and security. Throughout his career, Sarginson has focused on ensuring that businesses deploy secure, low-friction solutions that enhance both the overall business enterprise and user experience.

References

1. Watson, Bob. ‘Coronavirus and homeworking in the UK labour market: 2019’. Office for National Statistics, 24 Mar 2020. Accessed May 2020. www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019.
2. ‘A flexible future: Brits expected to call time on office life after lockdown’. O2, 6 May 2020. Accessed May 2020. https://news.o2.co.uk/press-release/a-flexible-future-brits-expected-to-call-time-on-office-life-after-lockdown/.
3. Lister, Kate. ‘Work-At-Home After Covid-19 – Our Forecast’. Global Workplace Analytics. Accessed May 2020. https://globalworkplaceanalytics.com/work-at-home-after-covid-19-our-forecast.
4. Lyons, Kim. ‘Google saw more than 18 million daily malware and phishing emails related to Covid-19 last week’. The Verge. 16 Apr 2020. Accessed May 2020. www.theverge.com/2020/4/16/21223800/google-malware-phishing-covid-19-coronavirus-scams.
5. ‘Advisory: Covid-19 exploited by malicious cyber actors’. National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cyber security and Infrastructure Security Agency (CISA), 8 Apr 2020. Accessed May 2020. www.ncsc.gov.uk/news/covid-19-exploited-by-malicious-cyber-actors-advisory
6. ‘The 2020 State of Password and Authentication Security Behaviours Report’. Ponemon Institute/Yubico, Feb 2020. Accessed Aug 2020. https://cdn.brandfolder.io/53ZDUYE6/at/g6ouqr-299a60-7a3pm1/Ponemon_Infographic_2020-UK.pdf.