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.
sovereignty. To do this in a changing world means providing the appropriate options to comply with local, regional and global regulations. The clear need is for solutions that are built from the ground up to provide flexibility around how and where data is collected, stored and analysed.

**GDPR compliance**

It has now been over two years since the GDPR came into force and the dissolution of the Privacy Shield framework shows that European Courts are clamping down on organisations that are not taking adequate steps to protect the privacy of EU citizens.

While the move most certainly does not mean that US organisations need to sever ties with their European partners, it does mean they need to review contracts, business processes and controls, and ensure that SCC implementations meet GDPR requirements. And, more importantly, that they are being properly exercised when data is being transferred, stored and processed.

Privacy is an extremely important issue for organisations and it is something that can impact a brand, disrupt the customer experience and tarnish a company’s reputation, if not done well. Therefore, organisations need to embed privacy into the roots of everything they do. This means approaching systems with privacy by design in mind and integrating considerations of privacy issues from the very beginning of the development process – whether for products, services, business practices or physical infrastructures. On the upside, there is an opportunity to differentiate by being a privacy champion: today’s consumers will respond to this.

Part of this means ensuring that cloud partners meet GDPR requirements and that they are not mishandling data or conducting transfers which could put them in breach of regulations. Organisations, therefore, need to identify cloud partners that are also practising privacy-by-design, ensuring that privacy and data protection is a key consideration in the early stages of any project and through its lifecycle.

Privacy rights are still emerging globally, but any organisation that is leading the way and championing privacy will have a significant advantage over its competitors. There is a great business opportunity for companies to address privacy issues now and it is much better to address privacy proactively, rather being summoned to court for taking the opposite stance.

It is time for CEOs and C-level executives to drive the importance of privacy throughout their organisations and start building data protection into their products and business practices. This includes partnering with organisations that have similar values.

The privacy revolution is upon us and honouring customer privacy and security is essential for any business to survive and can even give us an edge if done early and often.

**About the author**

Sam Curry is CSO at Cybereason. He is a security visionary and thought leader and has published broadly as well as being regularly quoted in the media on security trends and threats. Previously, he was CTO & CISO for Arbor Networks (NetScout) and was CSO and SVP R&D at Microstrategy in addition to senior security roles at McAfee and CA. He spent seven years at RSA (the security division of EMC, where he was a distinguished engineer and Fellow nominee) as CSO, chief technologist and SVP of product. Curry also has 24 patents in security from his time as a security architect, has been a leader in two successful start-ups and is a board member of the Cyber security Coalition, of SSH Communications and of Sequitur Labs (in the IoT security space) in addition to a number of advisorships across the security spectrum.

**Reference**

1. ‘British Airways fined £20m over data breach’. BBC News, 16 Oct 2020. Accessed Jan 2021. www.bbc.com/news/technology-54568784.

---

**Securing the remote workforce in the new normal**

John Grimm, Entrust

The Covid-19 pandemic has been the catalyst for accelerated worldwide enterprise digital transformation. It created an unprecedented requirement for increased digital capabilities just to ensure that businesses could continue to operate. The speed at which the virus spread and its impact on the way we had to live and work forced companies to act quickly, in many cases prioritising temporary functionality over security to simply survive.

Now, with government recommendations making remote working the norm rather than a passing phase and a majority of executives and office workers expressing a preference to continue to work some of the week from home even after the pandemic, the question then arises of how security can meet the demands of the modern workforce.
New ways of working

Global lockdowns and isolation precautions introduced a greater need to enable a workforce to leverage remote working and new ways of working to save jobs. However, this trend isn’t a new concept. The European Commission found that over the past 10 years companies had slowly been adopting remote-working capabilities for their staff as a resource for occasional use or to allow flexibility when office work wasn’t possible.¹

“The process of implementing temporary measures to enable this dramatic surge in remote working has put existing IT infrastructure under increased pressure and the security community has raised strong concerns”

The Commission highlighted that although only 5.4% of European workers were completely remote, an additional 9% (by 2019) spent a share of their time working from home. The challenge arises from the fact that now at least 40% of the European workforce is working from home full time, a volume for which most organisations couldn’t have prepared.

The process of implementing temporary measures to enable this dramatic surge in remote working has put existing IT infrastructure under increased pressure and the security community has raised strong concerns that this could endanger business and personal security. In Entrust’s ‘2020 PKI & IoT Trends Study’, when asked about security trends and capabilities, half (51%) of respondents reported that the solutions already in place either were incapable of supporting new applications or that there wasn’t the ability to change legacy applications.²

This is a concerning finding, considering the new demands on enterprise security systems caused by a growing remote workforce. It is not just the sheer number of people now requiring remote authentication and digital capabilities that are putting IT infrastructure under pressure. There are significant security challenges that face people working from home. Unsecured Internet connections, personal devices accessing business systems and the presence of smart home appliances put new stresses on business cyber security.

Internet of Things (IoT) devices are a volatile variable in the frontline of cyber security, with recurring stories about coffee makers being used as network points of entry and speaker systems used to record conversations. A majority of the IT security professionals surveyed in the report shared this concern, ranking the altering of a device’s function as the most important threat to IoT security, closely followed by the unauthorised control of devices. The glaring security concerns are exacerbated by the surge in ownership of smart appliances and connected devices, with nearly 25% of

Percentages of staff in various industries that in 2018 – before the pandemic – usually or sometimes teleworked. Source: European Commission.

Areas expected to experience the most change and uncertainty. Source: Entrust.
UK homes possessing at least one IoT-enabled device and projected ownership rising to nearly 50% by 2025.\(^3\)

**Attack surface**

These factors expose businesses to a greater attack surface than ever before. And with enterprise data being transmitted at an ever-greater rate, existing systems are, in some cases, unable to ensure adequate security. This could lead to data being stolen and sold on the dark web that, according to IBM, costs a business on average over $3.8m.\(^4\) A breach of any size can also lead to the exposure of intellectual property and damage to public trust with lasting impacts on business reputation.

The pandemic may have long-reaching permanent effects on the composition of the workforce in the future. Four in five chief executives expect remote working to become more widespread in their businesses as a result of Covid-19, with 72% of workers indicating they would like to work from home for two days or more on a permanent basis.\(^5,6\) This sort of operational transformation would necessitate major investment in security infrastructure such as PKI technologies to ensure authentication, access control and data protection. In fact, the data would suggest that budgets and resources are an area that 21% of IT security professionals ranked as the area expected to experience the most change and uncertainty.

**Being prepared**

The significant cyber security threat posed by remote working and businesses engaging in digital transformation programmes led to many IT security professionals implementing infrastructure changes in preparation. In fact, the data would suggest that the rapid increase in issued digital certificates for cloud applications and enterprise authentication is related to organisations creating the infrastructure for remote working and increased digital capabilities as 2020 began. This allowed some businesses to quickly move to a more digitally orientated work style: however, other organisations implemented quick fixes and temporary measures to meet the requirements of the time.

In the UK, businesses outperformed many of their international counterparts with their existing digital security capabilities before the lockdown enforced transition to a remote workforce. Nearly nine in 10 (87%) UK businesses already had an internally hosted certification authority that could authenticate identities and issue security certificates for enterprise applications.
UK enterprises also ranked highly with the number of certification authorities per organisation (fourth in the world) and the number of applications that require this sort of authentication (third in the world). This existing infrastructure ranks the UK as the world leader in internal certification authorities and perhaps indicates the technological advancements the UK has made, with a wealth of technology companies calling the UK home.

**Called into question**

Even with UK businesses’ impressive level of preparation and digital capability, these unprecedented times have called many security systems and protocols into question. Being better than a majority of the international community is an achievement, but it may not be enough. Secure solutions must be implemented at all levels to ensure network integrity and to cover technical gaps that remain in the UK enterprise landscape that may be magnified by the conditions of the pandemic.

However, the Entrust study would suggest that the technology itself is not the main concern in terms of security. Statistically, the largest hindrance is a lack of understanding of the capabilities of PKI – with 52% of respondents ranking this as the top challenge and 63% reporting that organisations may not have a clear idea of who is responsible for PKI ownership.

Organisational issues such as these are amplified by the distinct lack of resources and skilled individuals available to IT security teams around the country, with nearly half of UK respondents suffering from insufficient resources and skills. This is a global issue, however, and a considerable challenge to ensure the security of a growing remote workforce.

**Attracting attention**

The challenge of working from home has elicited the attention of various consultancies, with Deloitte suggesting a shift toward measuring success with data to ensure continuous improvement and professional services organisation EY redefining the work/life balance.

However, the real challenge is implementing security measures that can ensure that the new normal is as safe as it possibly can be.

The Entrust survey respondents highlighted the importance of deploying PKI solutions that can manage a greater range of organisations’ applications and implementing an effective certificate revocation technique on a global scale.

Even though the UK outperforms its international counterparts in terms of PKI deployment and security, there is clearly a distance to cover for the remote workforce to be entirely secured. While not a quick fix, organisations should look closely at the applications that consume certificates from their PKIs and ensure that the PKI is deployed with security measures that match the risk profile for the organisation and the applications.

Organisations could also implement stringent guidelines and training programmes to employees to raise the issue of connected device security and instil best practices to reduce human error in maintaining network integrity. As remote working becomes more common, even post pandemic, these actions are a must for businesses to secure a growing digital workforce and protect both the organisation and the employees.

**About the author**

John Grimm (@johnrgrimm) has extensive knowledge of the cyber security market with a particular interest in cloud security and the Internet of things (IoT) and is responsible for security strategy at Entrust. He has more than 25 years of experience in the information security field, starting as a systems and firmware engineer building secure cryptographic key distribution systems for government applications and progressing through product management, solutions development and marketing leadership roles.

**References**

1. ‘Telework in the EU before and after the COVID-19: where we were, where we head to’. European Commission, 2020. Accessed Jan 2021. [https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf](https://ec.europa.eu/jrc/sites/jrcsh/files/jrc120945_policy_brief_-_covid_and_telework_final.pdf).
2. ‘2020 Global PKI and IoT Trends Study’. Entrust/Ponemon Institute, 2020. Accessed Jan 2021. [https://drive.google.com/file/d/1SY08QK6_f3hrfigW1Fdn1sQ5TBhrDQNH/view](https://drive.google.com/file/d/1SY08QK6_f3hrfigW1Fdn1sQ5TBhrDQNH/view).
3. ‘Smart Home’ Statista. Accessed Jan 2021. [www.statista.com/outlook/279/156-smart-home-united-kingdom](www.statista.com/outlook/279/156-smart-home-united-kingdom).
4. ‘Cost of a Data Breach Report 2020’. IBM Security. Accessed Jan 2021. [www.ibm.com/security/digital-assets/cost-data-breach-report/](www.ibm.com/security/digital-assets/cost-data-breach-report/).
5. ‘Four-fifths of CEOs expect COVID-19 to entrench remote working – PwC’. Reuters, 11 Aug 2020. Accessed Jan 2021. [www.reuters.com/article/uk-health-coronavirus-work-pwc/four-fifths-of-ceos-expect-covid-19-to-entrench-remote-working-pwc-idUKKCN2562RH?edition-redir=uk](www.reuters.com/article/uk-health-coronavirus-work-pwc/four-fifths-of-ceos-expect-covid-19-to-entrench-remote-working-pwc-idUKKCN2562RH?edition-redir=uk).
6. ‘It’s time to reimagine where and how work will get done’. PwC, 12 Jan 2021. Accessed Jan 2021. [www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html](www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html).
7. ‘Increasing organisational resilience in the face of Covid-19’. Deloitte, Mar 2020. Accessed Jan 2021. [https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-future-of-remote-work.pdf](https://www2.deloitte.com/content/dam/Deloitte/global/Documents/About-Deloitte/gx-future-of-remote-work.pdf).
8. ‘Why remote working will be the new normal, even after Covid-19’. EY, 8 Apr 2020. Accessed Jan 2021. [www.ey.com/en_be/covid-19/why-remote-working-will-be-the-new-normal-even-after-covid-19](www.ey.com/en_be/covid-19/why-remote-working-will-be-the-new-normal-even-after-covid-19).