cpl.thalesgroup.com

THALES

Building a future we can all trust

2021 Thales Data Security Directions Council

The Evolving Role of the CIO

Welcome to a Slightly Altered Future

by Ashvin Kamaraju, Global Vice President, Engineering and Cloud Operations, Thales

In my role as an executive working in the cloud space, I am accustomed to change. I have seen many memorable developments over the past few decades, but nothing has caused such a tumultuous bump in the road as the coronavirus pandemic. Up until the dawn of 2020, the world was cruising along its timeline reasonably predictably. But the events that then unfolded substantially altered our perspectives on technology, work, life, and society – much more quickly than we are used to.

As a result, to help CIOs look ahead and envision the altered future that awaits companies and the people who work for them, we asked a group of experts to weigh in specifically on how the CIO role has changed over the years and especially through the pandemic period, and how it is predicted to change further. It is my pleasure to present this report with some of their thoughts.

Prior to joining Vormetric, Ashvin spent four years as General Manager and Vice President of Engineering at Symantec Corporation, where he led the development of a portfolio of enterprise storage software products. Earlier in his career Ashvin worked at Sun Microsystems as a member of the technical staff and as an engineering manager where he contributed to the Solaris operating system software for SPARCstations and led the development efforts for file and proxy cache servers. He has a MSCE and a master's degree in mathematics and computer science from the University of Cincinnati.

Ashvin is currently the CTO and Vice President Engineering for Data Protection at Thales, where he drives the technology strategy for Thales' data protection solutions, leading a global organisation of researchers and technologists that develop the strategic vision for the company's portfolio of industry-leading data protection products and services.

Previously he served as Vice President Global Engineering at Thales eSecurity following its acquisition of Vormetric. He led a geographically distributed engineering organisation that developed a broad portfolio of leading-edge data security products which met rigorous security standards, and which were designed for deployment in the enterprise, private, and public clouds.

Ashvin is an experienced leader with a proven track record, having more than 25 years of software development experience with domain experience in storage management, operating systems, big data security, encryption, and key management.

linkedin.com/in/ashvinkamaraju

twitter.com/AshvinKamaraju

Contents

Council Members

Ellen Boehm, VP of IoT Strategy & Operations, Keyfactor

Ellen leads the product strategy and go to market approach for the Keyfactor Control platform, focusing around digital identity security solutions for the IoT device manufacturer market. Ellen is passionate about IoT and helping customers establish strong security implementations for the lifecycle of their overall IoT systems.

Ellen has 15+ years' experience leading new product development with a focus on IoT and connected products in Lighting controls, Smart Cities, Connected buildings and Smart Home technology. Ellen has held leadership roles in Product & Engineering at General Electric and Sky Technologies over her career.

in linkedin.com/in/ellen-alkiewicz-boehm

Sherif Fouad

Sherif Fouad has been selected as one of the top CIO's within the Middle East in the year 2019 and 2020.

He has strong track records of exceptional overall performance in a fiercely competitive environment. Sherif is a strategic technology executive with proven success in delivering cutting-edge solutions in alignment with business strategy, utilizing far-sighted vision coupled with notable innovative abilities to modernize business operations, reduce technology risks, transform into the digital era and enhance customer satisfaction.

Sherif has led and implemented an IT transformation, innovation and technology refresh; including bank data center modernization, Built and executed bank digital strategy, applied DevSecOps, designed and deployed technology enterprise architecture, Application Development, Business process management and digital banking.

in kw.linkedin.com/in/sherif-fouad-ramadan-596b3522

Troels Oerting, Chairman of the Board of the World Economic Forum's Centre for Cybersecurity (C4C)

Troels Oerting is currently the first head and Chair of the Global Centre for Cybersecurity (C4C) established by the World Economic Forum in 2018 to mitigate the global challenges to security, privacy and integrity imposed by the Digital Transformation and the Fourth Industrial Revolution, by engaging and curating global stakeholders in a world-wide platform for prevention, protection, and prosecution. He has been working in cybersecurity first line for the last 38 years and has held several significant posts both nationally and internationally, resulting in an extensive network covering both public and private institutions.

As an expert in cybersecurity, Troels has constantly been looking for new legislative, technical, or collaborative opportunities to efficiently protect privacy and security for users of the Internet. He has pioneered new methodologies to prevent crime in cyberspace and to protect innocent users from losing their digital identity, assets, or privacy online. He enjoys a robust professional network covering the US, the EU, China, Russia, the Middle East, and Africa. He is a highly sought-after presenter and moderator on cyber-related issues and has participated in numerous conferences globally.

He is the cyber advisor for the EU Commission and Parliament and has also acted as a permanent delegate in many governance organisations including INTERPOL, ICANN, ITU and The Council of Europe. His skills as an advisor in cyber-related issues have been made use of by several governments and organisations and were instrumental in the establishment of the GDPR.

Troels is currently Chair of the Advisory Board to Denmark's Board Leadership Society Centre for Cyber Competences, and Chair at Bullwall A/S, Board member at several International companies and external lecturer on CBS Executive and Board Education in Cybersecurity. He is also finalising the establishment of a Cyber Risk Simulation Centre for Board Members in Denmark and abroad.

in linkedin.com/in/troelsoerting

twitter.com/TroelsOerting

Rick Robinson, Principal and Trusted Advisor at Goldbug Technology Consulting

Rick is the former Offering Manager for Encryption and Key Management for the Data Security Group at IBM Security. He is a regular speaker at IBM conferences and a contributor to SecurityIntelligence.com.

Throughout his career he has worked in the defence, retail, financial, manufacturing, communications, and data security industries, addressing the changing needs of information security and analytics. He has consulted with customers on security and key management architectures for security data at rest, data in transit, and data in use, for real-time and high-velocity applications, with a particular emphasis on problems that involve PKI and the use and management of certificates and SSH keys.

Rick has authored or co-authored thirteen patents, many in computer security and cryptography. Rick holds a Bachelor and Master of Science Degrees in Electrical Engineering as well as an MBA. In addition, he holds certifications from the Information Systems Security Certification Consortium (ISC)2, is a member of the Storage Network Industry Association /Storage Security Industry Forum (SNIA-SSIF), participates on the OASIS-KMIP technical committee, is a past Section Chair of IEEE, and past participant in the IETF. Amongst other volunteering activities, he chairs the election committee and manages bi-annual elections at K-12 school in Colorado.

Rick is currently operating his own consulting company, an active member of the Government Blockchain Association (GBA), and the host of the GBA Podcast – "The Future of Money, Governance, and the Law."

in linkedin.com/in/rrobinson256

www pod.co/the-future-of-money-governance-and-the-law

www securityintelligence.com/minimizing-the-encryption-blast-radius

Arthur van der Merwe, Information Security and Industry Compliance Manager at Australian Payments Network

Arthur van der Merwe is the Information Security and Industry Compliance Manager at the Australian payments self-regulator, Australian Payments Network (previously APCA). He is also a member of the International Association for Cryptologic Research (IACR), AsiaCrypt, IEEE and Australian Information Security Association (AISA) while conducting active doctoral research on authenticated encryption, leakage resilience and mathematical modelling.

He is also an active member of ISO, serving on the technical committees for Financial Services, security, and cryptography (TC68/SC2/WG13 and TC68/SC2/WG11). He serves on Standards Australia, Technical committee IT-005, Financial Transaction Systems, and is editor of the AS2805 suite of Standards. Arthur is also a Technical Advisory Board member of the Payment Card Industry Security Standards Council (PCI-SSC), participating in industry standards development for the PCI-PIN Standard, S3 Framework, Mobile Security (SPoC and CPoC), as well as the PCI-PTS Standard, PCI-HSM Standard.

in linkedin.com/in/arthur-van-der-merwe

twitter.com/AusPayNet

From the Frying Pan into the Fire

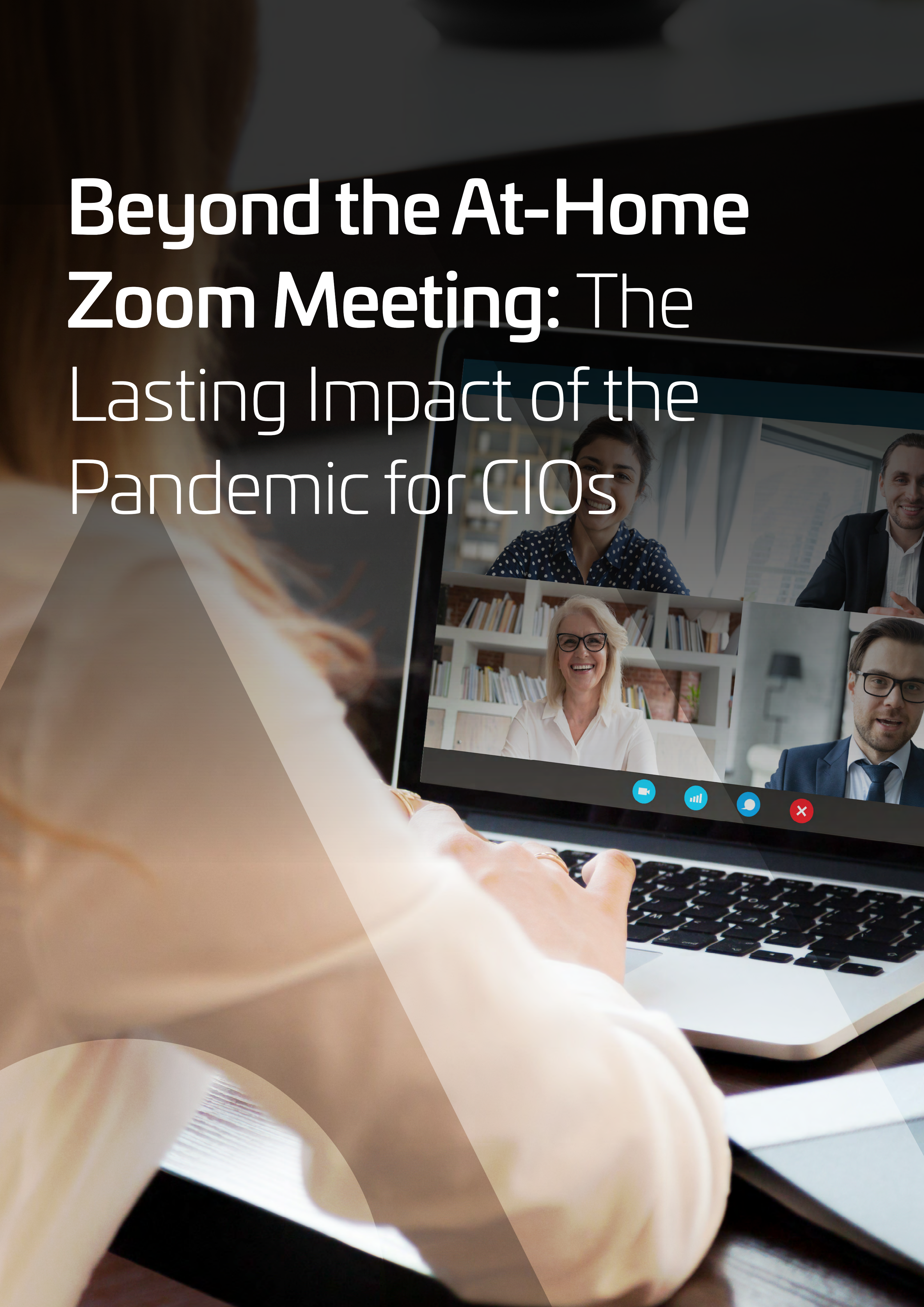
Even prior to the world-changing events of the coronavirus pandemic, the definition of the chief information officer (CIO) had already begun to change as the business environment around it evolved. With internet-facing technology taking an increasingly dominant role in the day-to-day operations of the typical organisation, the number of C-suite acronyms charged with overseeing its various elements (security, mobility, legacy technologies) grew correspondingly. The CIO had to work with the CTO (chief technology officer), the CRO (Chief Risk Officer), the CCO (Chief Compliance Officer), as well as others who had not yet achieved officer status, but whose roles tended to overlap or even conflict with the CIO or each other. These additional positions include IT Manager, IT Director, Director of Technology, Chief Information Security Officer (CISO), Director of IT, and Interim CIO.

In an era of constant, high-speed change, it can be difficult to determine, even within a clearly defined hierarchy, exactly who takes charge of, and is responsible for, an event such as a data breach or a ransomware attack. These are just two of the many activities that demand fast action to defend the organisation, restore its functionality and reclaim ownership of the data.

The CIO still has a unique and highly valuable role to play, one that is evolving while remaining focused on clear goals. The CIO balances responsibilities with the CTO, typically by looking inward, aiming to improve processes within the company, while the CTO looks outward, using technology to improve customer-facing actions. As such the position is moving quickly from being an administrator to becoming a trusted advisor to the rest of the company, while at the same time, liability for the outcomes of breaches and attacks is increasing among C-level positions, as evidenced by a September 2020 report from Gartner.

Such is the context in which we found ourselves as we posed our questions to the experts.

Beyond the At-Home Zoom Meeting: The Lasting Impact of the Pandemic for CIOs



How did your typical working day change when the pandemic hit, and how might this affect the CIO's future?

The overnight shift from people working in the office to working from home was "unprecedented, and led to an array of challenges for leaders, especially those who did not yet have a fully developed remote work policy, and who had not yet set up the equipment, security, and procedures to support one," says Arthur Van Der Merwe. Employees discovered that their workday was different now; commuting time was largely non-existent for those whose work could be done on computers, while those who still had to go to the office encountered empty rooms and shuttered cafeterias. Those who were thrust into the work-from-home mode had to learn how to interact through video chat while answering the demands of family and household.

Time seemed to become elastic. The lack of physical proof of a person's busy-ness such as being in a meeting, or visibly on the phone, meant that calls and meeting requests started to spread out across the entire day.

The CIO had to hustle to coordinate a team and IT organisation, to meet the needs of staff who still had to communicate, collaborate, and find space for impromptu brainstorming sessions and formalised meetings from their homes. Council moderator, Ashvin Kamaraju pointed out that there were also physical demands such as virtual private network bandwidth capacity and the dangers involved in opening up the workflows to give all employees access to assets on the corporate network.

> "Lockdown didn't really make the day shorter because the pressure was to work longer. A lot of people had the assumption that you're always available. For some it felt less like working from home and more like living at work."
>
> Arthur van der Merwe

In terms of a CIO's role in the future-of-work in the post-pandemic new normal, Troels Oerting looks to the future, in which a hybrid work scenario is the new norm. But, he says, "although self-directed work may become more feasible as people grow into their work-from-home skills, how do you create loyalty to a workplace that you have never been to, and how do we make sure that we create this bonding within a workspace so that people will not cheat or be negligent?"

> "How will we manage to recruit people in the future who we might never see in an office?"
>
> Troels Oerting

Troels' question about cheating is not aimed at the standard leaders' conundrum of "how can I tell if my employees are actually working at home," but instead focuses on security.

"With a trusted role like a security practitioner," Troels says, "it becomes quite difficult with staff who have access to the crown jewels; and not just the security people – it's all those who have access. In a bank, for instance, this means having admin rights to the SWIFT platform – the most delicate parts of your company's work." This, he says, is a fundamental breeding ground for cybercrime, easier even than social engineering, since remote, faceless individuals are given the opportunity for access with fewer reliable safeguards in place.

This opens a Pandora's box for the CIO: the spectre of having to pay employees, such as those who hold admin rights, a bonus to show up in person at the office, to cover the inconvenience of travel. This is the type of concern that would never have been considered prior to the pandemic lockdown, but increasingly, workers are clearly stating they would rather quit than be forced to return to full-time-on-premises work. The tech sector is already experiencing a significant shortage of skilled labour, meaning that the best and brightest have the option to work elsewhere – where, how, and when they want, and this gives them the upper hand in the travel-to-the-office-bonus debate. "This is a new challenge," Troels says, "that will fall into the CIO's lap."

Did you observe that in locked-down work situations, normal planning and approval procedures improved, degraded, or stayed the same?

Planning and collaboration in-line with established business processes would seem, in theory, to be easily translatable to a virtual environment. But Ellen Boehm points out just how much of this relies on in-person human relationships.

"For application development and software development teams, they are more used to working in person, going through agile processes, scrums, and stand-ups, for example. Or just being able to be right next to the developer. In an open office space, you can hear people chatting amongst themselves throughout the office as they try to solve problems and that's pretty impossible online. I think that from a development standpoint the whole product team had to shift the way they did that, and have it become a little bit more prescriptive."

Outside of the DevOps environment, Ellen suggests the same type of human contact is essential to the sales process, too. "Building a relationship with somebody over a dinner, or even just the five minutes before the meeting starts, those sorts of connections are what make business successful. Being able to know that you are going to buy a technology or invest in your cloud strategy with someone that you trust because you've had that in-person experience – you've broken down that barrier."

This delivers a new or updated challenge to the CIO: how to establish a culture in which these kinds of interactions can continue, formal (scheduled meetings) and casual (impromptu chats), in virtual as well as post-pandemic real world scenarios. Currently, virtual online spaces either seem dull, as with the typical video chat call, or too much like gaming and not serious enough. But the reality is, the need for interaction online will only grow. The bandwidth now exists that can remove the requirement for travelling for at least some activities. The lessons learned from the 2020 lockdown will be instrumental in improving the virtual interaction experience, and it will soon become as indispensable to working life as the smartphone already is. Tomorrow's CIO will be central in blending these new technologies with workplace processes.

> **"Lining up to get a sandwich or a coffee, those sorts of connections are what make business successful."**
>
> **Ellen Boehm**

How did the coronavirus pandemic impact your company's existing digital transformation plans?

Prior to 2020 many CIOs would have discussed digital transformation in terms of shifting work towards mobile, digital technologies, creating a world in which people could work from anywhere, using their laptops and coffee shop WiFi through a VPN. Further inside the B2B sphere, companies could offer personalised as-a-service solutions based on big data, artificial intelligence, and speed. Those things were all well in place prior to 2020, and the transformation was coming along reasonably well.

> "Working together in the same room is a great thing, but it's not necessary. The element of mobility is now what is implied with the concept of digital transformation."
>
> Rick Robinson

But there were other activities, too. Rick Robinson describes how one of the digital transformation plans at his former organisation was to consolidate their campuses around the specialties of teams. If a person worked in Marketing they were expected to relocate to the town where that campus was going to be. "If you weren't willing to move, that meant you had to find another group to work for."

The pandemic-induced necessity for people to work remotely stopped these types of plans quite quickly and have since not only turned large organisations away from the idea of practice-specific regional campuses but are also posing even more pressing questions about floor space in general. Many are now considering reducing their physical footprint, especially in high-rent areas, as the digital transformation focuses, internally at least, to a hybrid work environment in which hoteling and hot-desking replace dedicated cubicles.

There are other elements of digital transformation that get less airtime in discussions and planning sessions but carry significant weight regardless. One of these is data and specifically, its storage life. Cloud technology opened up a seemingly infinite capacity to store data of all types. As a perfect demonstration of Parkinson's Law colliding with Moore's Law, cloud storage capacity expands to handle the data available, and the value of this storage ability seems to increase exponentially as more devices get connected to it.

> "The next step in digital transformation is having a way for the data to be sanitized."
>
> Rick Robinson

Rick Robinson suggests that organisations should start to put a lifecycle on their data, meaning that "the data has to be sanitized at some point." He suggests that "although the quarterly reports of a corporation from 2001 will always and forever be known, individual transactions that were created from individual customers from 2001, their names, phone numbers and email addresses should, and likely need to be anonymized, redacted, or completely erased." This substantially transforms a company's attitude and approach to the management of archived output that has been built up over years, decades, even centuries.

Robinson acknowledges that deleting information causes people a great deal of worry. "Accountants," he says, "will say, 'you can destroy anything as long as you make a copy of it first,' which defeats the purpose, but reflects a common mindset."

Stored data might seem to be an asset, retrievable when needed, but it is also a sitting duck for cybercrime. Data includes passwords, home addresses and other personally identifiable information (PII). Even if passwords expire and are replaced, the data remains useful for brute force attacks, password spraying, and social engineering efforts. This argument was at the centre of a recent case involving Facebook, which dismissed a scraping event of the PII of 500 million subscribers in 2019 as "old data." High profile breaches, such as RockYou2021 in which 8.4 billion passwords were leaked in June 2021, reveal that data, even if stored, has value, and maintains the potential to be used and abused for decades to come.

Robinson suggests encryption of stored data, down to the granularity of individual files may be the answer. "When every document is encrypted under its own key, if you compromise one document, one piece of information, one PowerPoint, one record in a database, that gives you no advantage in compromising anything else in the database," he says. This alleviates much of the worry over stored data since the cost of decryption would not make it worth a bad actor's time to steal.

David Friend, co-author of The Bottomless Cloud, argues the other way, that archived data should not be destroyed. Refuting the cliché of data being the new oil, he suggests instead that it is currently a friction because of our inability to manage and access it effectively, paired with the energy costs required to store it. He pictures a world in which storage costs no longer impede progress, and in which organisations will transition into a post-industrial era that focuses on the limitless abundance of data. He suggests that by 2035 we will have access to over one yottabyte of data – one billion petabytes, and the near-zero storage costs of this data will spur new, innovative business models.

Friend suggests that data should be kept even if we see no immediate use for it and should not be destroyed simply due to cost. Troels Oerting has spoken at, and hosted events at the World Economic Forum, in which the CEOs of the thousand largest companies on the planet convene to meet, talk, and learn. He notes that digital transformation will empower countries that have been hitherto denied access to the expensive infrastructure of the PC era. These countries, he suggests, will leapfrog the PC era entirely, to instead leverage mobile technology, capitalising on 5G-enabled devices and the internet of Things (IoT). "More than 50 billion IoT devices will connect to the Internet, and 80% of these will never speak to a human being but will instead communicate machine-to-machine."

> **"You probably don't want to be first movers in this area. You probably want to be a fast follower."**
>
> Troels Oerting

In studying and planning for these, a CIO can also look to countries that have already achieved significant progress in digital transformation, such as Japan – which installed inexpensive broadband internet connectivity to almost all homes and businesses twenty years ago – or Abu Dhabi's Smart City initiative, which among achievements has normalised the use of facial recognition technology for commerce and for public safety. Sherif Fouad points out that Kuwait's Boubyan Bank started its digital transformation many years ago and its strategy of growing and serving its customers led to it being named best digital Islamic bank for 2019 and 2020. Boubyan Bank increased its investment in digital transformation during the pandemic, with all customer operations maintaining high availability and no interruption to the customer experience.

This expansion of data, connectivity, "as-a-service everything," and the resultant growth in cybersecurity needs, will all become part of a CIO's expanded responsibilities.

Data Security Rebooted

How has data security and cybersecurity changed in the past five years?

"CIOs are in the unique position of overseeing their company's cloud policy from a strategic and functional level, and over the past five years or so, the industry, collectively has placed great reliance on cloud providers and cloud technology without fully understanding how a particular provider works," says Arthur van der Merwe. Cloud has made itself attractive due to its apparent cost-effectiveness and scalability, but issues of technical and physical security, along with the credibility of cloud service providers themselves remains of significant concern.

A recent fire in a cloud facility in France revealed just how wide these gaps may be, given that the fire had a physical cause (a faulty uninterruptable power supply), and that a.) the data lost was resident on bare metal servers within the facility and not the cloud itself, and b.) the clients who lost the most had not backed up their company's data independently. These are the types of issues that go well beyond the simple functionality of the cloud and should never vanish from a CIO's ToDo list.

Ashvin Kamaraju points out that the past five years have shown expansion in threat detection including the use of artificial intelligence in threat hunting, incident management and malware detection. Concurrent to this, however, is the increase in more sophisticated attacks including social engineering, which was the cause of the Twitter hack of June 2020, and supply chain attacks, the most infamous of which (to date) is SolarWinds/Orion.

Ellen Boehm adds how over the past five years, the IoT and its industrial sibling IIoT, have revealed abuses of technologies such as cameras, including doorbells and nannycams. These, she says, are "driving elevated awareness around security as well as the liability that they bring, not just to developers and manufacturers of the devices, but to those who use them."

> "There's a lot of misconception about cloud environments and security. People don't really know what the adequate controls to put in place are."
>
> Arthur van der Merwe

Troels Oerting suggests that these various threats, which have each become so powerful in the past few years, necessitate a consolidation of the concept of security. "It's old-fashioned to talk about physical security, information security and digital security," he says. "Security is security, since it is all interlinked already."

"Nobody wants to be that next news story."

Ellen Boehm

Perhaps the most poignant example of this is ransomware. In 2020, there were 65,000 ransomware events in the U.S. alone, which averages out to seven every hour. This has emerged as a highly lucrative business for organised cybercriminals, not only in its relative ease of deployment, but in their increasing sophistication around issues such as setting ransoms based on their research of an insurer's willingness to pay.

Ransomware has evolved from being a crime against a company to becoming a part of the cost of doing business. It hits companies daily. In the first quarter of 2021, the most infamous cases included Colonial Pipelines, which resulted in near economic catastrophe by closing down fuel deliveries to the entire US east coast, and Ireland's health service, which faces months of disruption as it continues to recover from a May 14 ransomware attack.

Troels Oerting suggests it is "idiotic to say 'never pay the ransom'" because this must be weighed against the time and cost of decrypting and restoring backed up data (if there is any), which is seldom easy or quick, and comes at a substantial cost.

"Tabletop exercises should create eye-opening moments for the board."

Troels Oerting

The CIO is in prime position to initiate tabletop exercises with other senior officers to determine, for example, the rationale and even legality of paying ransoms between countries, establishing plans for bolstering against repeat attacks, what the corporate culture is or should be regarding negotiating with and/or paying ransomware pirates, as well as gathering intel on significant corroborating factors, such as the reality that much cybercrime success comes from deployment on days of the year when a target company is minimally staffed, such as on the eve of, and during national holidays. This goes well beyond technology and moves into issues of staffing and year-over-year project planning.

In addition, there are always new developments for the CIO to learn about and translate to the rest of the organisation. For example, a recent Thales Data Threat Report shows that among plans to deploy new access mechanisms as a result of pandemic-induced changes such as increased remote work, 44% selected Zero Trust network access/software-defined perimeter as their leading technology. (Zero Trust implies that no devices are to be trusted, even if they are part of a corporate network). This narrowly outpaced cloud-based access management (policy-based access, authentication and single sign-on delivered from the cloud) at 42%. Conditional access, where access decisions are evaluated on richer context around users, location, threats, and activity, was a very close third at 41%[1].

The CIO is in prime position to be able to translate the often-ethereal notions of cybersecurity into real-world visuals, such as the spill over effects that a breach would have on a company's brand, reputation, share price, litigation, lost customers, environmental issues, and much more.

[1] Link to: 2021 Thales Data Threat Report – Global Edition (p.9)

What Lies Ahead?

What do you see as data security/cybersecurity priorities for the next five years?

The future of data security will be a place where companies no longer wish to be alone in the trenches but will elicit far more cooperation, to face the criminals en masse, and in which cloud providers will similarly be forced to be more transparent in their operations, say Troels Oerting and Arthur van der Merwe. In short, there will be a need for greater cooperation, inside and out. The CIO will need to coordinate the IT department, all of whom are working under the pressure of strict deadlines, to think about the solution and threats more holistically, and will need to elicit more knowledge and collaboration from suppliers and competitors.

Five years is a long time, and it is guaranteed that technology and cybercrime will continue to advance in this period, as with any other. But with incremental increases in communication such as 6G replacing 5G as well as advances in artificial intelligence and machine learning, it will be up to the CIO to redefine the job to ensure there is a balance between administration and ongoing learning.

Ashvin Kamaraju puts it succinctly: "It takes time for decision makers and organisations to come to grips with change, and with technology, because it is not solely about products. It's about a core set of principles. These must be implemented cautiously and within the constraints of how the company works. Legacy systems, both technological and cultural, cannot support change too quickly."

> **"Change is not a button, it's a knob. If you turn the knob too far clockwise too quickly, you impact productivity and negatively impact stakeholders."**
>
> **Ashvin Kamaraju**

Where do you see cloud strategy heading in the next few years?

Cloud technology is not a single thing. Since its deployment, debate has bounced between public, private, and hybrid cloud setups. Hyperscalers like AWS, Microsoft and IBM have become the choice for many organisations, but CIOs need to continue to keep their eye on contingencies. Isolated incidents such as fibreoptic cables being accidentally cut by a backhoe, or a supply chain bottleneck outage as happened with content delivery network agent Fastly in June 2021 reveal weaknesses that make even a well-managed cloud temporarily useless when their customers cannot access it.

Cloud strategy stretches across the floor from IT to the C-suite. Beyond the technical vulnerabilities lies issues of subscription management, data residency, ownership of data encryption keys, and much more.

Much of cloud culture today echoes the "Big Blue" mindset that made Microsoft the dominant player in desktop PCs, by latching itself to the traditions established by IBM in the 1960s and 70s. As such there were far fewer Apple computers in offices across the world. These same values permeate the decision-making process when choosing a cloud service provider. IBM and Microsoft remain part of the old guard in the information technology space, while relatively newer companies like Google and Amazon, might appeal to decision-makers whose early professional years coincided with these companies' growth. Similarly younger, more localised cloud services may appeal to younger managers, based on a comfort level that goes beyond physical features and benefits and speaks to their own evolving mindset.

The fact that all three of the dominant cloud providers are essentially American might also shift the decision needle as companies based elsewhere in the world seek to diversify their data storage, comply with regional data protection rules, or simply work with local cloud companies whose collection of offerings matches or exceeds what they have experienced with the big three.

> **"In my experience, almost three quarters of CIOs are now identifying cloud first or cloud migration as the top digital transformation for this year."**
>
> **Ellen Boehm**

The CIO Crystal Ball Reveals “Divesting, Diversity and Distributed”

How do you see the role of the CIO changing in coming years?

As mentioned above, the CIO is surrounded by other types of digital officers, which doesn't render the position obsolete, but does demand that it becomes more cross-functional. The position also needs to be less top-down, diluting the command-and-control siloed architecture that was forged in the previous century. As Arthur van der Merwe suggests, "the future CIO must become a force that drives the digital transformation, rather than just focusing on how it works."

Ashvin Kamaraju points out, younger employees might not be eager to adopt a company's standard issue laptop with its adherence to a large ERP system. They may instead prefer using cloud-based apps on their own devices for communication and collaboration. These are people who are highly aware of their value in the marketplace, their career mobility, and the independence this brings. They will not be able to understand an organisation that chooses email over group collaboration apps, any more than a company that expects all its employees to return to the office full-time.

For a CIO, this is still a good place to be, says Ellen Boehm. "CIOs are going from managing costs, driving efficiency, and focusing on internal operations, to being more involved, more visible and more strategic in terms of growing the business by leveraging technology. There's a lot that can be brought to the table when it comes to things like supply chain integrity and implementing this zero-trust mentality, and that's where I see the CIO heading."

"Divesting responsibility might be the key after all," Rick Robinson adds. Rather than being threatened by the other titles circling the CIO's office, he feels the extra talent will be needed, with the CIO position's traditional responsibilities broken down and distributed among the people who focus on either protecting the company against attack or leveraging technology to be competitive.

The concept of a CIO being a Chief information executive remains valid but requires a step away from outdated notions that it must be fixed in its role and stature. As a position that holds responsibility for internal processes centring around digital transformation, Troels Oerting suggests that the ongoing qualifications for this position be kept evergreen and fresh, meaning that instead of requiring a 10-year education for the position, the focus should be on more recent education in areas such as computer science and cybersecurity, paired with significantly higher levels of human "soft skills" that allow for improved communication skills and the ability to transfer technical and strategic concepts across the organisation and at all levels.

The examples mentioned above, such as handling the quickly advancing pursuit of ransomware payment strategies show the need for an individual who is well-schooled in the political machinations of business, but who retains up-to-the-minute knowledge of cyber-related threats and developments, to fill this seat.

> "The modern CIO has to be very forward-looking in terms of shifts and trends from the newer generation. You can't attract the right talent and retain them with old school ideas."
>
> Ashvin Kamaraju

> "We in security are not promoting fear. We are protecting hope."
>
> Troels Oerting

> "It is the transformation of CIO, from an exclusive technical provider to a business leader."
>
> Sherif Fouad

Where do you think the CIOs of the future will come from?

According to Rick Robinson, there are two ideal markets for finding individuals for the future CIO position. First are the well-established educational institutes within a country's military structure, such as the Air Force, which is well-known for its cyber security organisations. People coming out of the Air Force with a recent cybersecurity skill set would be ideal candidates for CIO positions, he says.

The second market that Robinson suggests is the hacker culture itself, specifically the person who may have been a hacker during their 20s, but who has matured and who has grown tired of breaking things and is now more interested in preventing things from being broken. This individual's maturity comes from a short lifetime of looking at the world from the perspective of how to break in. This approach is alien to the traditional C-suite career ladder, but a person from this world brings several key skills that seldom see the light of day in conventional education.

Conventional education teaches from collected experience and often packages solutions and thinking patterns in a logical sequence, as in, "you can't learn algebra until you have learned basic mathematics, you can't compose music until you have mastered scales, you can't go into management until you have studied management theory, and you can't hire employees until you understand Myers Briggs." This approach tends to condition people to see and think along the lines of their education and nothing more. Take SQL injection as an example.

SQL injection is an old but still useful hacking technique in which malicious SQL database code is placed inside an entry field on a form. The code is then essentially injected into the system to perform its mission. It is likely that every CIO already knows what a SQL injection attack is. The point of this analogy is a person who has been taught to think in a certain direction sees a "surname" field on an online entry form as a space where only a surname should go. But a hacker sees that same form field as rife with possibilities and will create malicious code to fit into that "surname" field. A hacker sees potential where linear thinkers cannot, and this is in large part why today's hacks and breaches continue to succeed, even with educated cyber specialists on staff. The mindset of the hacker has not been constrained by traditional education. It challenges everything and sees every challenge as an opportunity to break something or achieve something.

Many hackers, when interviewed, will say things like "I just tried this action to see what would happen," and these same hackers readily admit seeing their parents recoil in fear at the mere thought of clicking on a function button out of what might happen. And therein lies the generational rub. Adults, especially those whose formative years happened before the internet explosion of the 2000s cannot help but be imprinted with an analogue fear of consequence: "don't press that, you might break it." Because in a hierarchal culture, breaking something means getting into trouble.

> **"I have never let my schooling interfere with my education."**
>
> **Mark Twain**

This is why many younger executives of unicorn companies prefer to hire people who appear to be more like them: aggressive, unafraid, and part of a highly connected, non-linear culture, that grew up in an age of unfettered access to information and a dissolution of hierarchical structures. You can see this even at the pinnacle of technological achievements in the unconventional methods of new-age innovators like Elon Musk whose YouTube videos of landing used Space-X rockets on floating barges – even the failures – turned the vastly siloed space industry on its head.

These new executives look for the "right fit" people first, and train necessary skills into them after hiring. A computer science education might provide good background wisdom, but does not provide an edge over a 20-year old when it comes to understanding the impact of, for example, Ethereum as a viable system of smart contracts and decentralised finance for next-gen banking.

The third source of tomorrow's CIOs that Robinson identifies is indeed the higher educational facilities – colleges and universities, but to do this, these organisations must continue to rethink their own curricula, admissions requirements and online/on-prem teaching techniques to attract and produce the type of skilled professional who can meet the challenge of becoming a CIO.

Sherif Fouad reaffirms that the time is long overdue to level the playing field to become more proactive in terms of diversity, equity, and inclusion (DEI), which brings with it distinctive opinions and life experiences that can best enhance security posture and defences. "The key difference now," he states, "is that the advancement of the work-from-home model has proven that it is feasible for security specialists to achieve some or all their work remotely. Lockdown, was, in essence its proof-of-concept."

People whose schedules require a split between work and family commitments (childcare or parent care, for example) would now no longer be excluded from the workforce. Those who have mobility challenges that make daily commuting difficult are now much more accessible, as are those who live in towns outside a traditional commuting belt – essentially anywhere in the world. This also connects the world to younger employees who may still be studying at school or who do not yet have the financial independence to move out. Further, it offers terrific opportunities for those with social challenges such as being on the autism spectrum to learn to integrate comfortably into corporate life. The talents of all these individuals can now be drawn into the mix without distance, or even physical presence being a complicating factor.

The distributed teams model is the archetype for the post-pandemic economy, says tech executive and author Alberto Silveira. In his book, Building and Managing High-Performance Distributed Teams, he explains that the distributed teams model is an improvement upon remote work in that no team member is made to feel that they are an outsider working from home while the rest of the group is together in the office. Silveira's approach is that when everyone connects to a virtual space from somewhere else, and that there is no central boardroom, teams get the best benefits of diversity and group dynamics simultaneously.

> "If every university on the planet only generated technical expertise and engineers – computer science majors, cybersecurity engineers and the like, they still would not satisfy the global demand for the next 100 years."
>
> Rick Robinson

How is the skills shortage in security-related disciplines impacting your own business/your clients' businesses?

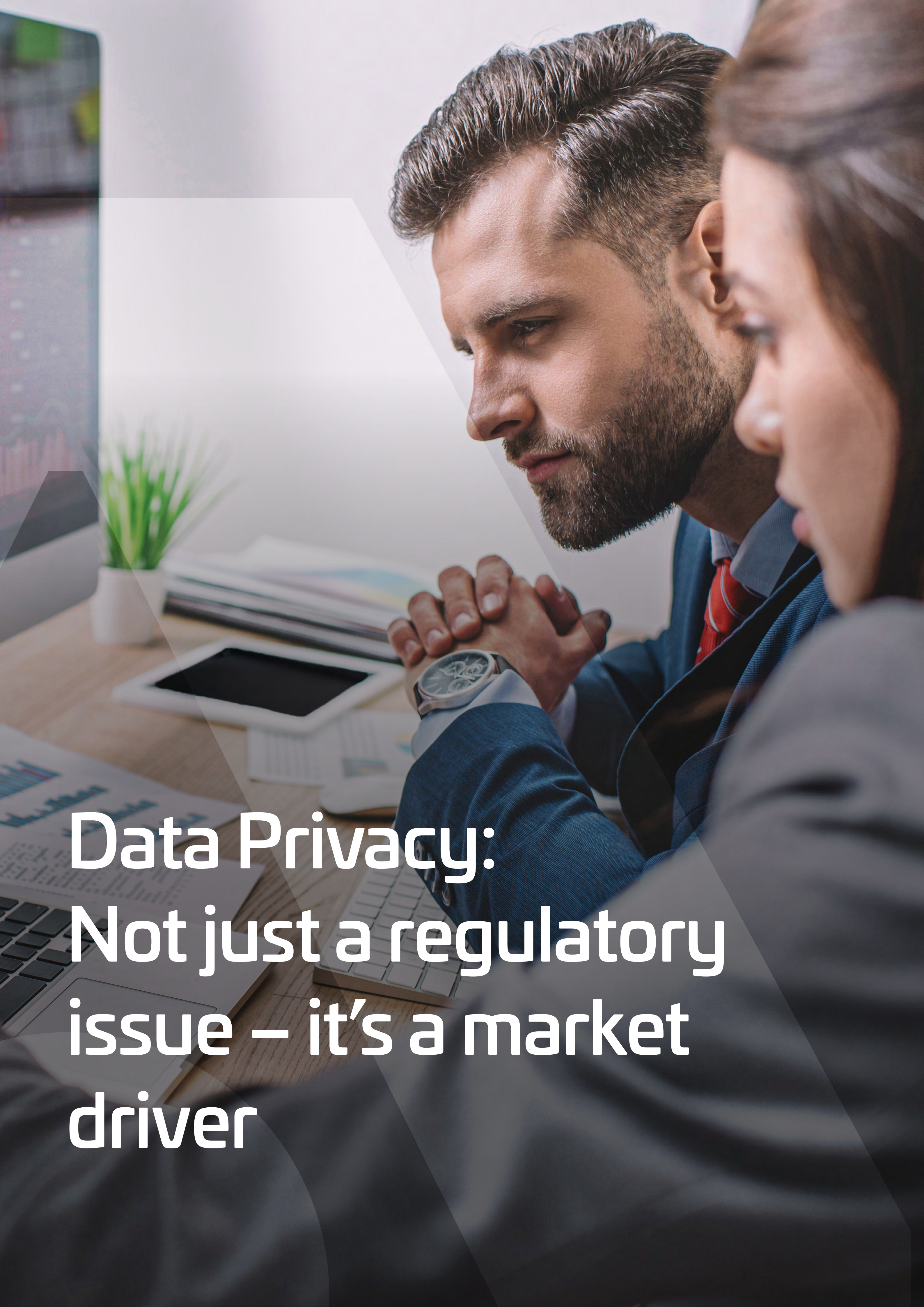
There is a global shortage of skilled professionals in security, and this is impacting tech businesses as well as their clients' businesses. But this is not just one type of shortage but three. "The first is due to people already in the business choosing to stay within their existing roles, or staying with a specific technology, such as AWS, Google Cloud, or IBM," says Arthur van der Merwe. This creates a shortage of talent through a lack of vocational ability and breadth. There is also a significant amount of fear and reluctance among IT people to shift to new skills.

At the same time, as previously mentioned, companies that are not able to accommodate the demands of professionals concerning flexible work, smart work, and remote work, will experience a shortage not because there are no skilled workers available, but because the company's existing culture does not appeal to what these workers expect and demand. This issue promises to paint itself large upon the landscape as the millions of people who have now experienced work-from-home start to demand it all- or part of the time.

Granted, not every CISO or cybersecurity specialist can stay home one hundred percent of the time – sometimes it is necessary to be present where the machinery is. But as Alberto Silveira points out, the workplace of the immediate future is one in which the talents of team members need to be overseen and embraced by a more socially aware type of leadership. "The best talent for your teams may be located anywhere. This also means they may have different definitions of what work-life balance looks like. Leaders who refine their attitudes toward geography, skills, lifelong learning, work equality, and other individual talents and soft skills, will succeed in building high-performance teams."

Rick Robinson points to the third reality, that the skills shortage exists because skilled workers have their pick of desirable jobs: "Absolutely anybody who's got the skills of either being a security architect, a strategist, or a person skilled in ethical hacking – they are all fully employed with offers waiting. I get pinged every other day with people desperate to find more resources, and this is causing wage inflation."

All these conditions give the CIO fertile ground to attract people according to their own sets of expectations, or to bring people in who may have no background at all, or who are at a disadvantage due to economic, physical, or geographical circumstances, but who have the attitude and a desire to learn. This is essentially out of the box thinking for a traditional C-level officer.



Data Privacy: Not just a regulatory issue – it’s a market driver

Are current and developing rules for securing information (GDPR, HIPAA, CPRA) sustainable in a globally connected economy?

The past few years have seen the emergence of regional regulations around the use of data and the protection of information. GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and the CPRA (California Privacy Rights Act) are perhaps the three most famous at present, and the rules behind them are being enforced, and penalties are being meted out.

But with regionalised protectionism comes a minefield of data storage and data sovereignty issues that the CIO must be aware of and then manage, not only for data at rest but also for data in flight. The well-intentioned concepts behind protection of personal data and the "right to be forgotten" fly directly in the face of global, centreless internet technology and cause major headaches for companies whose global presence must now be fractured to accommodate differing and evolving demands of individual nations, or subsets of nations, as well as legal judgements like 2020's Schrems II from the European Court of Justice, which had implications for the use of US cloud services. It is an essential de-connection of the internet.

There are concerns about the sustainability of GDPR-type legislation simply because what was written a few years ago may not be correct today or next year. For example, "how does the requirement for data to be kept within the borders of the country work in the case of encrypted data in which a portion of the encrypted data is in the country, but another portion is outside the country, or in a cloud elsewhere?" asks Rick Robinson. "How does the rule apply when both pieces are needed to reassemble the data? In a similar vein, it can be argued that regulations that were created for the telephone industry are no longer applicable, because a cell phone isn't a telephone: it does not use telephone lines, it does not have a central office, and it is not delivered exclusively by a telephone provider."

> **"Some of our customers are leaning towards saying 'I just don't want to know. That way, I don't need to collect it and then feel like I'm going to be violating something."**
>
> **Ellen Boehm**

These are examples of instances where regulations will struggle to be consistent with other regulations, with the legislative bodies that create them, and with the CIO who must integrate them into a company's culture and vice versa.

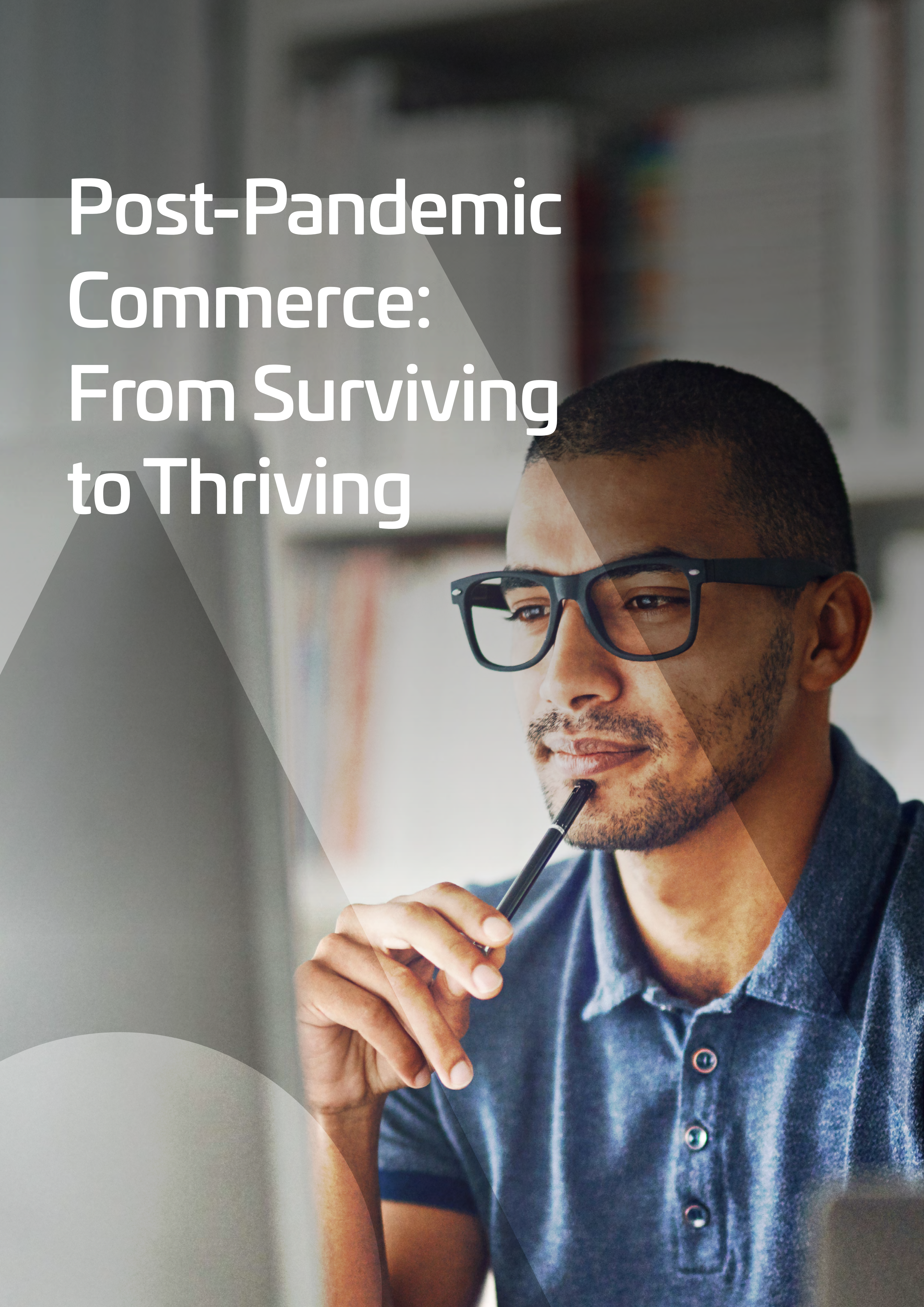
Furthermore, consumers in B2B and B2C markets are becoming more vocal about the protection of their own data and are willing to move their business if they feel they are not protected effectively. It has become part of their buying decision, alongside price and brand loyalty. They will be actively seeking out retailers and suppliers who can demonstrate superior approaches to data protection. It should be noted that every time customers are asked by a breached company to change their password, this becomes a perfect moment for the customer to consider cancelling the relationship.

It is becoming more widely understood, and reflected in reports by consultancies like McKinsey that "companies are responsible for the data they collect," which makes data protection a major consideration for consumers that interact with a brand.

In the US, the May 12, 2021 White House Executive Order in cybersecurity moved the influential American economy closer to cohesive cybersecurity legislation, as did the appointment of new leaders across a swath of security-related departments including the Cybersecurity and Infrastructure Security Agency (CISA)and the office of the national cyber director.

This means that oversight of data is gradually growing more mature, driven on one side by frequent and impactful breach incidents, and on the other by a growing recognition of the enormous ripple effect that data disruptions can bring. This is creating a necessity for legislators, insurance companies and enterprise to make more visible and tangible strides.

Post-Pandemic Commerce: From Surviving to Thriving



How do you see the shift to DevOps environments impacting a company's long-term stability?

The history of software development is one in which meeting the demands for speed, quality and security have had to balance against the culture itself, a culture collectively referred to as DevOps. There has been a movement to remove traditional production silos between the people who write code and those who test for quality, moving the testing process "leftwards" chronologically into the design phase, and redefining traditional roles along the way. This is not always greeted with enthusiasm by members of the software development lifecycle community. The responsibility for the appropriate and cost-effective rollout of DevOps and software in general will remain one of the primary responsibilities for the CIO in coming years.

> "Transformation doesn't mean someone will lose their job. But what will always be needed is a change to the approach of work to reflect a capacity to evolve."
>
> Sherif Fouad

Quality

The quality assurance mindset is another. One of the drawbacks of the increased speed of production overall is the corresponding increase in the speed of expectation on the part of the users who expect fast downloads, instant activation, and flawless performance, and who will stop using an app if these do not occur. This then results in organisations delivering a minimum viable product (MVP) into the market, which undercuts quality testing and improvement. "This happens when a company wants to be first to market and is under executive pressure to do so. It becomes a serious problem," says Ellen Boehme. "When implementing a new control system that will be operating a power turbine or a huge industrial asset, there needs to be tollgates, milestones and approvals, along with the time to think through its development."

Rick Robinson adds to this his image of the security blast radius, which refers to a compromise of any sort, usually failure of security technology or software. The job of a security architect should be to minimise the blast radius of an event. When a company has cut corners and now depends entirely on a single supplier, for example, then the blast radius becomes substantial if that component or that supplier is compromised and there are no other protective mechanisms in place. Although the security architect may be charged with the responsibility of understanding and minimising the blast radius, it will be up to the CIO to remain aware of the existence of this scenario and delegate the responsibilities of mitigation accordingly.

Quantum Computing

One of the great successes of data security, especially over the last two decades, is encryption. It has grown in strength and sophistication enabling the existence of floodgates against the relentless flow of cybercrime. This can best be proven by the fact that most cybercrime now focuses on penetrating a system through human operators, using spearphishing and social engineering, for example, meaning that cracking encrypted data has proven too costly and time-consuming for threat actors, who will generally always seek the easier route.

However, no ramparts can stand forever. Part of the CIO's role will be to continue to assess the opportunities and threats emanating from quantum computing. As Todd Moore writes, "while there is disagreement about the timeline, researchers

> "The second quantum revolution is coming"
>
> Todd Moore

and engineers anticipate dramatic advancements in quantum computing over the next five to ten years...current public-key cryptography solutions, which are developed using complicated mathematical formulas, provide reliable security based on the amount of computing power required to decipher them. It would take the world's most powerful computers thousands of years to crack these solutions by brute force. However, a sufficiently large quantum computer would be able to break the cryptography tools in a manner of days or even hours."[1]

A recent IDC report sponsored by Thales, shows that 26% of organisations globally are in the process of operationalising their quantum computing plans, or will do so in the next 18-24 months. As much as quantum computing threatens to weaken existing security protocols, the same technology can be used to strengthen the defences of the near future.

Blockchain

Increasingly, organisations are starting to contemplate a move to blockchain in the same way they did with the cloud over the past decade. Blockchain is a technology that uses a jury of connected computers to agree upon and then record the transaction entries on numerous identical copies of a digital ledger that are then encrypted in a way that makes decryption and alteration of the records exceedingly costly in computing resources, time, and money.

Blockchain is most associated with bitcoin and other cryptocurrencies, which is erroneous. Although cryptocurrencies do use blockchain for their mining and transactions, they are just one of a wide range of services and products that use it. Others include smart contracts, supply chain integrity, traditional financial transactions, vital document authorisation (birth certificates, passports, mortgages) and medical records, to name just a few.

In just the same way the concept of the cloud grew from a single, theoretical publicly available storage area, we have seen the development of private clouds and hybrid models, large hyperscalers such as Amazon Web Services (AWS) and Google Cloud, as well as more regional cloud service providers (CSPs) more suited for data sovereignty and digital protection regulations. With cloud, it was the technology that counted – infinitely scalable, highly adaptable, and economically attractive – as opposed a single brand or model. With blockchain, the same will emerge. Companies, especially financial institutions, will develop private blockchains, leveraging the encryption and archiving technologies without placing themselves out in the open. Other organisations globally will likely seek to benefit from its extensive reach, to protect investments and monies without the expensive, and sometimes corrupt, oversight of regional banks or governments.

Artificial Intelligence and Machine learning

A wide range of activities can be bundled into these terms but suffice to say their presence is being felt in all areas of business, from intelligent routing of deliveries to facial recognition. For every positive development there are equal and opposite negative ones, including deepfakes (counterfeit videos or audio recordings that appear impossibly genuine) and AI- and ML-enabled spear phishing/social engineering techniques that learn how to impersonate

[1] Todd Moore, Dark Reading draft

people and suppliers with great accuracy. Here again, both AI and ML can be deployed for attack and defence. As Ashvin Kamaraju stated, earlier in this paper, AI is already being used in threat hunting, incident management and malware detection.

Quantum computing and blockchain, AI and ML are all existing technologies, in their infancy perhaps, but by no means purely hypothetical. Thinking back to the summary of a CIO's position, looking inward while the CTO looks outward, this places the CIO squarely in the line of responsibility to continue to work with the CTO to fully understand, strategize upon, and then deploy these technologies in the interest of their company's future viability.

Last Words – Ashvin Kamaraju

In asking the questions of our experts, we ranged over several topics that themselves have been and will continue to be subject matter for papers in their own right. But what was evident from the experts' responses is that these new priorities and technologies that will form the future of business all require the input and influence of the individual holding the CIO chair.

Far from being a redundant and dated position, an organisation would better serve itself by taking time to redefine the position, delegating certain roles to other officers and managers, and continuing to ask the question, "how best can our CIO continue to look inward, aiming to improve processes within the company, while the CTO looks outward, using technology to improve or innovate products that serve the customers?"

The two roles are vital and are co-dependent. Holding them together is a bond of knowledge, based ideally on an upgraded combination of continuous learning and continuous communication, not just with each other, but with every member of the organisation. In just the same way that IT and Security are not departments to be hidden away in siloes, the conversation about security, processes and people must remain front of mind and leading edge. It is the role of the CIO to ensure this happens.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

THALES

Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <