BT

Pushing the Perimeter: How digital leaders are securing the dispersed enterprise

TechPros.

Contents

Introduction

What a difference a year makes. In March and April of last year, the pandemic changed billions of lives in many ways, including workers needing to work from home rather than their usual office.

Overnight, company networks moved from a centralised corporate space, protected by layers of firewalls, anti-virus software and hardware to an employees' kitchen table and home broadband.

Overall, organisations appear to have handled the sudden move to remote working well. However, most networks weren't set up to handle large scale remote working and such a rapid shift to the cloud and other types of digital technology.

Clearly, the changes in the shape of company and public-sector IT networks have big implications for cyber security.

It's unclear what, if any, long-term effects the pandemic will have on how and where we work, but a hybrid of cloud-based home and remote working with office and client site meetings seems likely. About four in ten UK employers said they expect more than half their workforce to work regularly from home after the pandemic has ended, according to research published last year by the Chartered Institute of Personnel and Development (CIPD)[1].

What does this rapid change mean for organisations' cyber security? Is there a risk that in the rush to remote and flexible working, and an increasing reliance on cloud computing, organisations are creating new IT security headaches? How are organisations handling the transition? Is there best practice? What are the main security risks of the new "perimeterless" network, and how can the risks be mitigated?

To find out we interviewed security and business leaders at organisations in various industries on these and other pressing security matters.

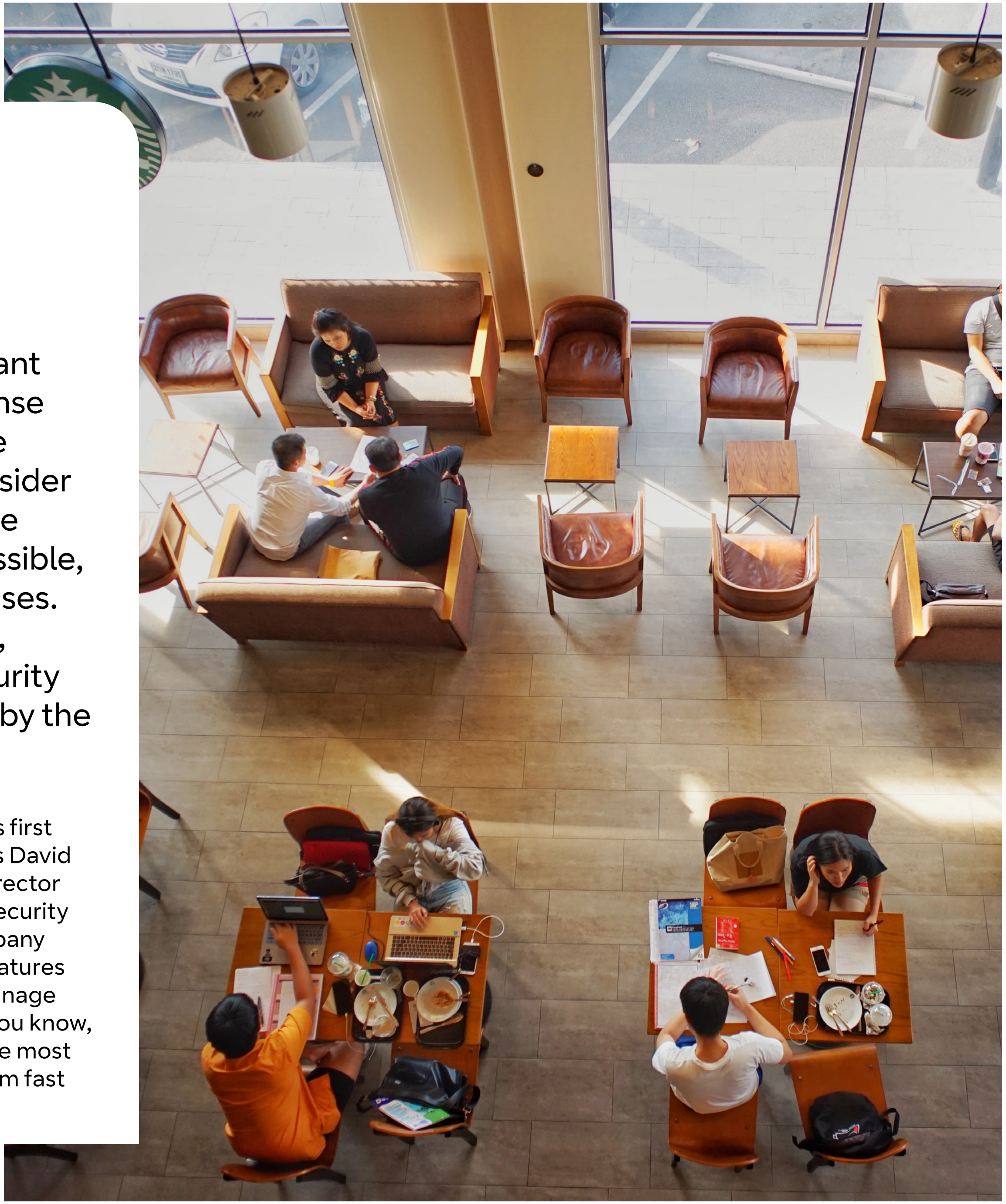
This eBook combines these findings with our insight to offer a guide to embedding the digital workplace into business strategy.

The race to secure flexible working

The move to remote and hybrid working is often reliant on cloud technology. Since March last year, in response to the pandemic, many businesses have had to make rapid shifts to the cloud without the time to fully consider the security implications. When the pandemic hit, the pressure was on to get the job done as quickly as possible, and this involved lots of workarounds and compromises. They didn’t have the time to do impact assessments, sometimes even having to relax or even remove security controls to address capacity constraints brought on by the break-neck shift to remote working.

Businesses that would normally only allow access to a cloud service via a company laptop suddenly had to allow access via personal devices, because all the company hardware was stuck in the office. And businesses that only wanted employees to access the corporate network through a VPN had to allow access via the cloud because they just didn’t have enough VPN capacity.[2]

“What keeps me up at night is first of all what am I missing?” says David Kosorok - Dynamic Senior Director of Application and Product Security at DocuSign, a software company specialising in electronic signatures and helping organisations manage contracts and documents. “You know, am I finding the things that are most critical? And are we fixing them fast enough?”



David Kosorok – speaking in a personal capacity and not on behalf of DocuSign – adds that organisations should do more than the bare minimum of, say, annual cyber-security training for its employees. "If you just do that, there is proven evidence that that is guaranteed failure, right?" Quarterly security training is more useful, he says.

Other technology and cyber-security executives we interviewed said that they were worried about growing security threats of "ransomware" – malicious software designed to block access to a computer system until money is paid to the cyber criminal – and attacks on suppliers in their supply chain.

In 2021 alone, six ransomware groups compromised 292 organisations in different industries around the world between January 1 and April 30, and potentially reaped just over $45 million, according to the [eSentire Ransomware Report](). In June, JBS, the world's largest meat processor was forced to [temporarily close its US meatpacking plants]() after it fell victim to a ransomware attack.

"The one thing that keeps me up at night is a complete wipeout scenario, the ultimate cyber crisis scenario is some sort of ransomware that takes everything down," says Jon Winbow - Director of Information Security at GlaxoSmithKline, one of the world's biggest pharmaceutical companies. "And we have to recover from a point where we have to bring everything back. And we've never been in that situation before."

Ophir Zilbiger, Global Head of Cyber Security Advisory, at accounting firm BDO, is also concerned about the growing threat from ransomware. It underscores the importance of an organisation having a resilient information security infrastructure, he says.

"In the last 15 years, cyber security protection has been king. Organisations have invested in checking firewalls and anti-virus software, in addition to different kinds of sophisticated mechanisms to prevent this or that. They've invested less on detection and response, and on resilience. They feel protected, because they bought security, or they invested in security. In reality, their organisations have some big gaps in their armour, such as protection from ransomware."

Some industries have become more lucrative targets for hackers during the pandemic. In the past year to eighteen months, the likelihood of a cyber-attack on the pharmaceutical industry has increased, especially on suppliers in pharma companies' supply chain, Jon Winbow adds. "One of our third-party suppliers was hacked about six months ago, and then we had to scramble around. Okay, what does that mean to us? What have they got? What do they do for us? Are we impacted? It's a huge issue and a massive concern for us."

Our conversations with business leaders about cyber security and new post-pandemic working patterns highlighted three key challenges.

Challenge 1: Secure your business from network to cloud

Legacy infrastructure issues are driving organisations to consider virtual, cloud-based network software. But many businesses aren't sure whether they can access the benefits of cloud working securely. A hybrid approach – part cloud/ part on-premise IT – could work for them. They're unclear about what security measures they need to support an effective hybrid workforce. They want to increase network flexibility and save costs with software-defined networking while protecting the business from risk.

Businesses face the challenge of implementing flexible and dynamic security to control global networks. They need to allow people to work from anywhere on mobile devices but protect them from identity misuse and endpoint threat.

User authentication is especially important for Lundbeck, a pharmaceutical company specialising in brain diseases.

"We're trying to make sure that we have a consistent multi-factor authentication policy across all cloud solutions," says Torben Olsen, Lundbeck's head of cyber security.

Finding workers with the right cloud security skills can be a challenge, he adds. "There is a skills gap when an organisation is trying to operate a cloud platform between many people who have been trained and used to an on-premise solution. Cloud technology works differently. You need different skills to build cloud applications and manage them."

> ***"We're trying to make sure that we have a consistent multi-factor authentication policy across all cloud solutions."***
>
> **Torben Olsen**
> **Head of Cyber Security at Lundbeck**

Challenge 2: Keeping up with the changing threat landscape

The impact of a security breach ranges from data loss, financial loss, fines from regulators and reputation loss. Compliance is a key issue. In some cases, chief information security officers (CISO) and the C-suite senior management are personally responsible for security breaches. Businesses face a challenge identifying and addressing ongoing threats in a cloud-based environment. Identifying security threats and mitigating threats needs to be an ongoing process, not a one-off exercise.

“User authentication is key,” says Karl Mozurkewich - Principal Architect at OpenText, which provides information management services and technology. “It’s a pillar of being able to identify who somebody is and what they’re allowed to do [in an organisation’s IT systems].”

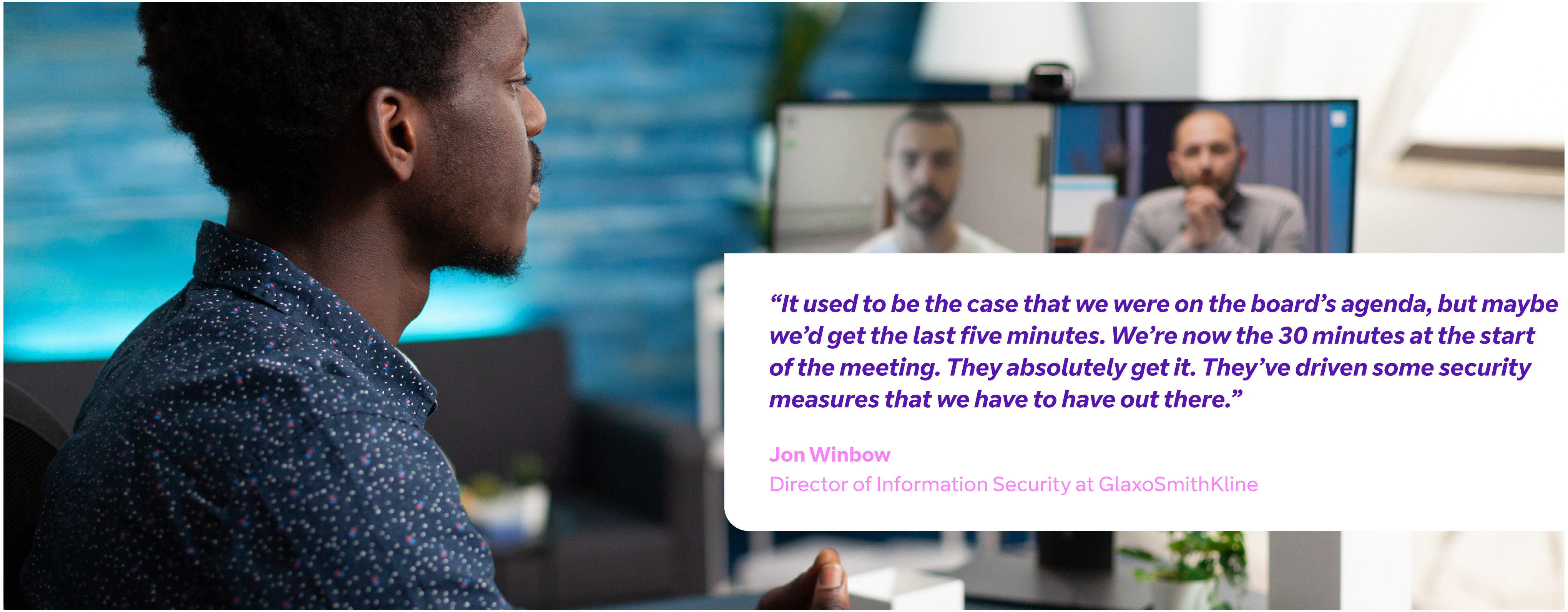
Security is a priority for any cloud migration project. After that has been dealt with, organisations can accelerate their move to the cloud by limiting customisation of their cloud software, Karl Mozurkewich says. It can help them finish cloud migration much quicker.

“What happened in the past year with Covid, and everybody shifting to remote work, was that a lot of organisations got caught flat footed,” he says. “So instead of over engineering large migration projects, they identified the 80% that really needed to get migrated or functionality.

Of course, no cloud project or decentralised corporate perimeter/network can be 100% secure. No matter how robust an organisation's IT security technologies and security policies are, they'll be of limited use if employees and suppliers ignore security guidelines and do things that could allow hackers into a company's network.

"Companies need to think about how much control they want over devices their employees use, workflows and data in the cloud, and how this impacts user experience and productivity," says Anmol Misra, researcher, and Director of Infrastructure Security at Autodesk, which makes software products and services for the architecture, engineering, construction, manufacturing, media, education, and entertainment industries. Anmol Misra, speaking in a personal capacity and not on behalf of Autodesk, added: "Companies must get used to having less control over devices and security. You need to rely on individuals, behavior, and culture in addition to automation if you want to be ahead of the curve. End-users play a critical role in the success of any security program."

> ***"Companies need to think about how much control they want over devices their employees use, workflows and data in the cloud, and how this impacts user experience and productivity."***
>
> **Anmol Misra**
> Director of Infrastructure Security at Autodesk



"It used to be the case that we were on the board's agenda, but maybe we'd get the last five minutes. We're now the 30 minutes at the start of the meeting. They absolutely get it. They've driven some security measures that we have to have out there."

Jon Winbow
Director of Information Security at GlaxoSmithKline

Challenge 3: Valuing cybersecurity

Sometimes the low-key success of IT security can undermine its perceived value. When cybersecurity is working correctly it's invisible. This can lead to a lack of perceived value, which in turn can make it hard to get buy in from the board/senior managers for some parts of the IT security budget. Businesses face the challenge of defining what good security looks like for them. And communicating the benefits to their board.

Boardroom attitudes to cyber security may be changing for the better, though. Technology executives we interviewed said that information security had risen in the board's agenda in the past few decades. The pandemic has underscored the importance of strong cyber security, especially when more employees are working from home.

"This pandemic has created a different way of thinking about information security, and we can't do the same things and expect different results," says Selva Vinothe Mahimaidas - CISO at Houghton Mifflin Harcourt, an education and learning company. "Our company has almost doubled the investment in information security spending as a percentage of our overall IT spend."

Other executives we interviewed echoed this view that the pandemic, and surge in remote working, had pushed cyber security even further up the boardroom agenda.

"It used to be the case that we were on the board's agenda, but maybe we'd get the last five minutes," says Jon Winbow of GSK. "We're now the 30 minutes at the start of the meeting. They absolutely get it. They've driven some security measures that we have to have out there."

How can organisations estimate return on investment (ROI) from cyber-security spending?

Cyber insurance premiums are sometimes a “forgotten element” of ROI calculations, says Donal Munnelly, Security Proposition Manager at BT Ireland. Having a robust Cyber security policy backed up by defence in depth can dramatically reduce your cyber insurance premiums, he says.

“Obviously, the costs to a cyber-attack depend on the nature of the attack. If the attackers target your critical business operations, there’s a huge cost to the business when output stops. If the attack has targeted sensitive information there can be additional fines levied by regulators that could be substantial.

“If intellectual property is compromised there can be a cost in terms of competitive advantage. Avoiding these costs are a substantial ROI for cyber security.”

Cyber security threats are changing constantly. Just keeping track of them could be a full-time job. C-suite executives are more interested in solutions. What technologies and security policies and procedures can mitigate security threats and, ideally, improve an organisation’s productivity? The exact security threats will be different in each organisation, but in our interviews with business leaders, a consensus emerged about what action organisations should take to secure their more fluid network perimeters and workforces.

> ***“If intellectual property is compromised there can be a cost in terms of competitive advantage. Avoiding these costs are a substantial ROI for cyber security.”***
>
> **Donal Munnelly**
>
> Security Proposition Manager at BT Ireland

Five actions to secure organisation networks and infrastructure

1. Focus on the endpoint

Securing today's perimeter-less networks demands a focus on endpoints. It's important to make sure that you have robust endpoint security that not only protects against known attacks but also includes detection and response capabilities to address new threats.[3]

When Security, IT Infrastructure and cloud teams are distinct, it makes a case for end-to-end security investments difficult. Organisations need a roadmap towards per-application user authentication – wherever their users are.

2. Make security drive the business

Security is often seen simply as a cost centre, but security technology can allow business transformation and cost savings.

"One of the things we do is we've benchmarked and looked across our peers at what everyone else is doing and constantly looking at where do we sit?" says Jon Winbow of GSK. "We also delve into our incident response. Are we missing anything?"

Taking quick and effective action after a cyber attack is discovered can save organisations money and protect their reputation, although putting an exact financial value on these things is tricky.

"Are there additional measures that we can take to help us to repel cyber attacks quicker?" says Jon Winbow. "It can be worth looking at the 'kill chain', where you really want to be repelling things early on an attack, rather than just as they're about to get your crown jewels. We're constantly looking at that."

Measuring your organisation's cyber security policies and performance against peers, and using cyber security industry standards and methodologies, such as ISO 27001, the International Information Security Standard can also help companies automate procedures and trim costs.

"Maybe you're seeing less incidents compared with your peers," says Jiang He, Risk Manager at financial services company Sun Life. "You need to continuously understand your own weaknesses and address these proactively," says Jiang He, Risk Manager at financial services company Sun Life. "One approach is to compare your security posture with that of your peers by using industry framework. Maybe you will realise that you are better than your peers in certain domains but lagging in others. Such evaluation would provide you with a good opportunity to identify your priorities moving forward."

"Maybe you're seeing less incidents compared with your peers. You need to continuously understand your own weaknesses and address these proactively. One approach is to compare your security posture with that of your peers by using industry framework. Maybe you will realise that you are better than your peers in certain domains but lagging in others. Such evaluation would provide you with a good opportunity to identify your priorities moving forward."

Jiang He
Risk Manager at Sun Life

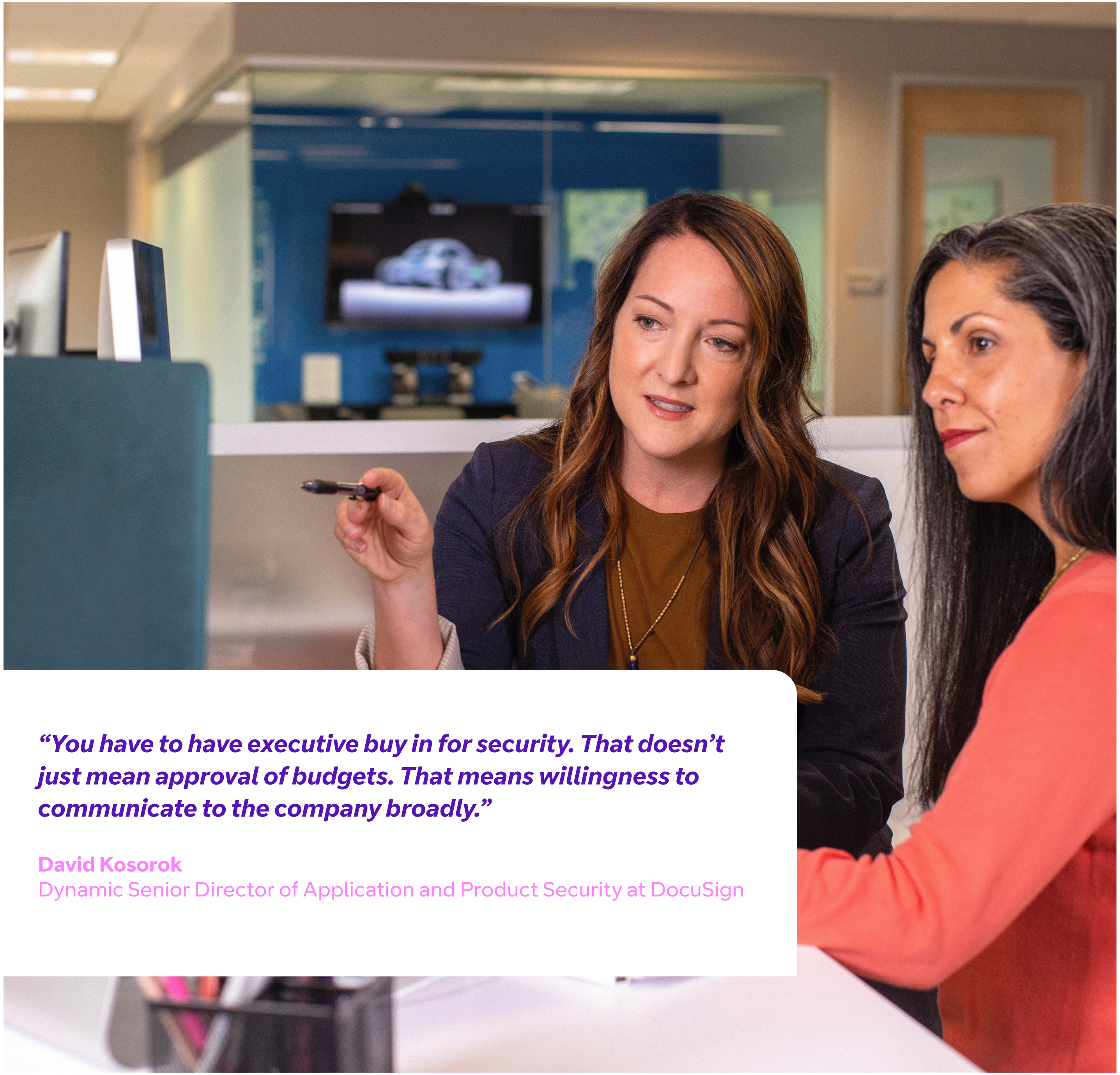
3. Measure success to drive board level buy-in

Measuring the success of your security is crucial to provide metrics to create a business case for investment. Security accreditation is one way to do it.

There's a need to address the disconnect sometimes seen between security reporting and translating that into actionable business context and ROI. Security professionals need to improve communication with the board to get the budget they need, and especially communicate the ongoing, not just one-off benefits of cyber security spend.

"You have to have executive buy in for security," says David Kosorok at DocuSign. "That doesn't just mean approval of budgets. That means willingness to communicate to the company broadly."

"For example, if a company's IT or security department educates other users in the company about the warning signs for "phishing" cyber attacks (misspellings, poor grammar etc.) and the number of successful phishing attacks falls significantly, because fewer employees open suspicious-looking emails. This benefit of improved IT security is worth communicating to the board, David Kosorok says. The CEO may want to personally email the IT/security staff involved, thanking them for helping to keep the company secure", he adds.



> ***"You have to have executive buy in for security. That doesn't just mean approval of budgets. That means willingness to communicate to the company broadly."***
>
> **David Kosorok**
> Dynamic Senior Director of Application and Product Security at DocuSign

4. Resource security

Resourcing network security with the right skilled staff is an issue that some businesses address by having different security partners in different countries – or by using managed services. In some cases, automating and enhancing infrastructure security technology can release IT and security staff to carry out work that adds more value.

“You don’t need 10,000 more tools,” says Anmol Misra of Autodesk. “To prevent most cyber attacks, we need to effectively use the tools we already have and do the basics, like logging, patching, hardening, or IAM hygiene.” Taking these and other basic security measures will work to protect your organisation.

5. Maintain ongoing security

Piecemeal, annual security training for employees just isn't good enough. There's a need for constant training and intel about threats and products. Business leaders need to continuously monitor their estate to spot breaches and respond quickly to alerts.

They need to get the basics right, such as pro-active security patching and integration of logs into their existing solutions. Then, they need to avoid data loss and to remain compliant as they migrate services to the cloud.

To maintain security, exercises such as "assume breach" – expecting a sophisticated attacker will find a way into your estate and manage to stay hidden for some time – can reduce the risk of an organisation becoming complacent about its IT security. Assuming the attacker is already inside changes your goal to making it harder for them to move about - and easier for you to detect. "Wargaming" (a simulated cyber incident focusing on how members of an IT department and other departments respond to an incident) can also be useful.

Now that many businesses have developed a highly distributed architecture, having visibility over their assets is even more important. "[Threat management](#)" services, the best of which combine security expertise, context-aware threat intelligence and tools to monitor (or even hunt for) and manage critical incidents can oversee your infrastructure and traffic to identify and deal with any suspicious activity that could indicate a cyber-attack.

Clarity over security threats and how to deal with them can help boost boardroom confidence in security technology and may bolster arguments for increasing security spending.

> ***"If given an immediate 20% increase in our information security budget, I would split the additional funds between spending on the "stability and integrity" of the company's IT systems and data. I'd spend the other 10% on researching more cutting-edge things, such as the best new cyber security technologies that we could use or adapt for our business. I'd focus on where our business is going in the next five years or so and any new cyber security threats on the horizon."***
>
> **Rodion Varynskyi**
> Director of Network Operations at J2 Global

If executives we interviewed were given an immediate 20% increase in their information security budgets, what would they spend it on? Rodion Varynskyi, Director of Network Operations at J2 Global, an Internet information and services company, says that he would split the additional funds between spending on the "stability and integrity" of the company's IT systems and data. "I'd spend the other 10% on researching more cutting-edge things, such as the best new cyber security technologies that we could use or adapt for our business. I'd focus on where our business is going in the next five years or so and any new cyber security threats on the horizon.

Conclusion

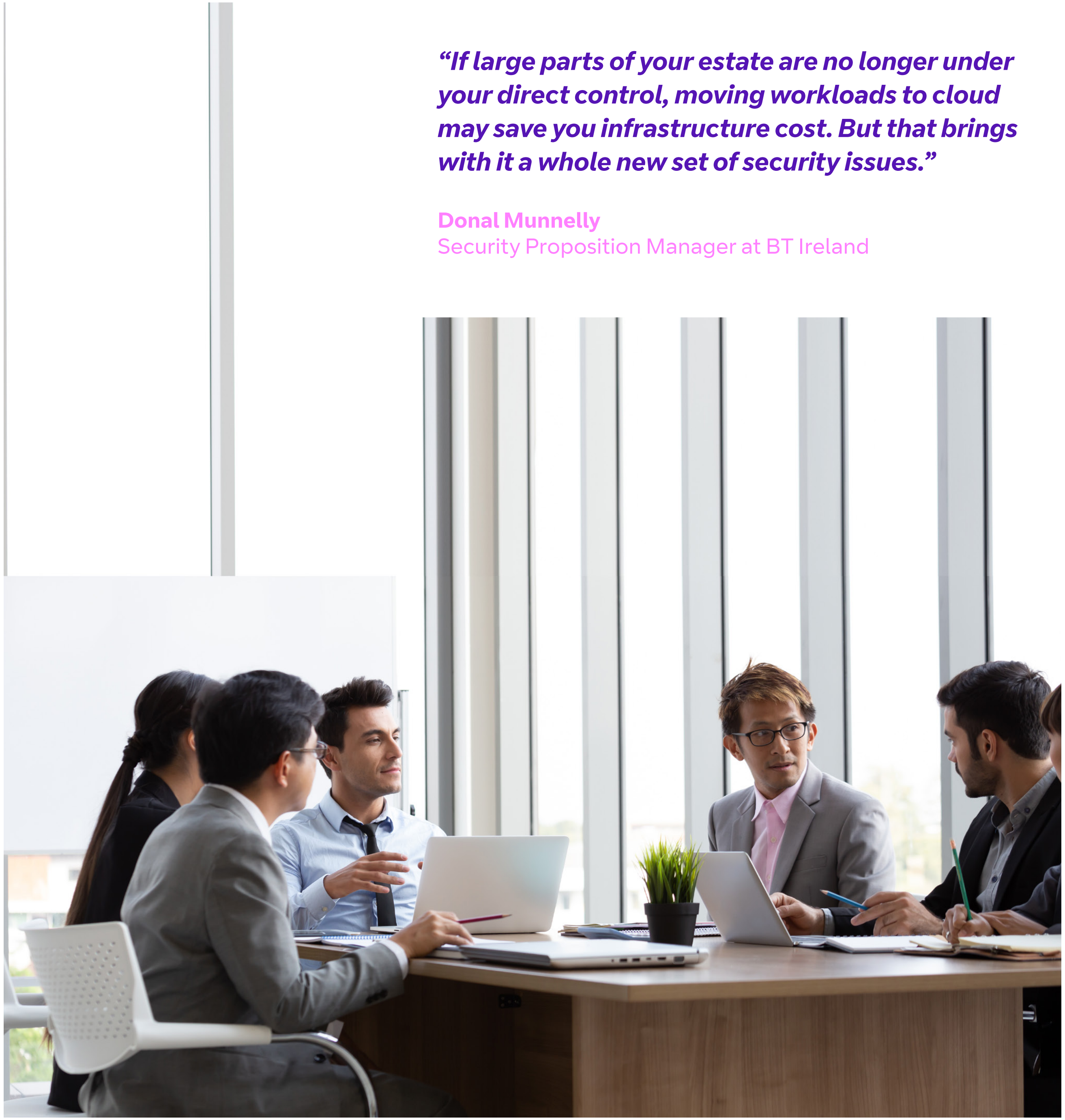
Security is now a business issue, not just a technology issue. Security has moved from an IT discussion to a boardroom discussion, yet there is still a reliance on the technical team to “make the business secure.”

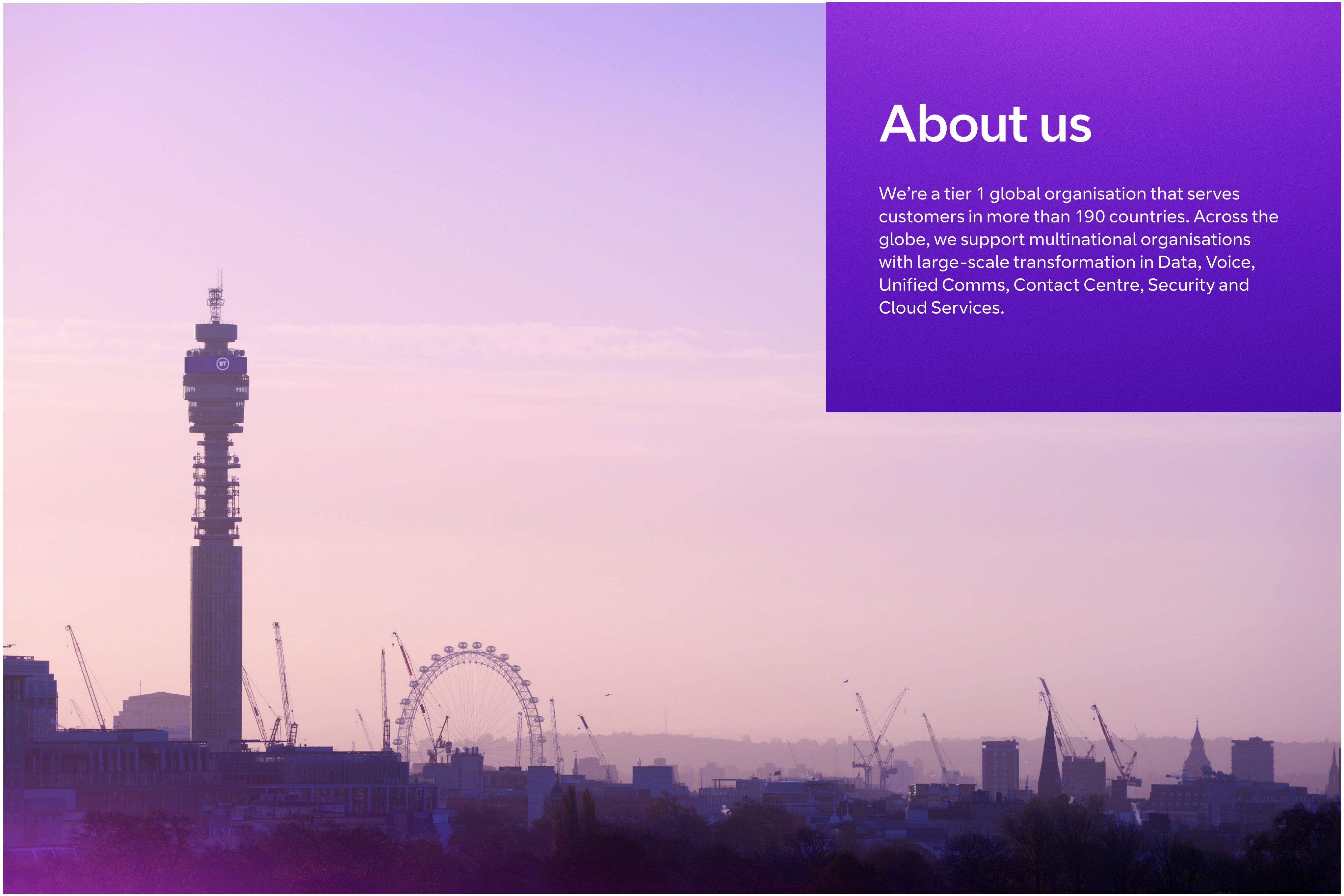
It’s no longer about the network perimeter. The adoption of mobile and cloud means you can no longer have a holistic view of your network perimeter security. Work is increasingly done outside of the corporate network which means loss of visibility of devices and locations trying to connect.

Remote working has become the new normal. It’s no longer just about maintaining remote access for a small portion of the organisation. Resources must be available 24x7 from anywhere, on any device.

“If large parts of your estate are no longer under your direct control, moving workloads to cloud may save you infrastructure cost,” says Donal Munnelly of BT Ireland. “But that brings with it a whole new set of security issues.”

> ***“If large parts of your estate are no longer under your direct control, moving workloads to cloud may save you infrastructure cost. But that brings with it a whole new set of security issues.”***
>
> **Donal Munnelly**
> Security Proposition Manager at BT Ireland





About us

We’re a tier 1 global organisation that serves customers in more than 190 countries. Across the globe, we support multinational organisations with large-scale transformation in Data, Voice, Unified Comms, Contact Centre, Security and Cloud Services.

Acknowledgements

This report benefits from the input of many industry leaders, who kindly shared their insights. We would like to extend particular thanks to those we have cited directly in this eBook, along with the numerous others who contributed more general insights towards the bigger picture.

Abbie Barbir
Senior Adviser at Aetna

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Aloysius Cheang
Chief Security Officer at Huawei UAE

Aloysius has two decades of experience in cybersecurity. He is the Chief Security Officer of Huawei UAE, responsible for driving the company's cybersecurity vision of building a safe and secure intelligent, connected, digital world in the UAE and the region. He is also a Board Director for US-based (ISC)2 and UK-based cyber leadership think tank, the Centre for Strategic Cyberspace + International Studies (CSCIS).

Antoine Bour
CSO at Huawei

Antoine holds CISSP-ISSAP, a high level certification in IT security from ISC2. He is number 66884, a number which is capable of completely managing all aspects of the security of an information system, designing and deploying a security policy for information systems at the most reasonable cost. A number that can train, guide or simply explain "Safety" to everyone: from senior managers to simple employees.

Ajitha Narayanan
Director Quality, Security and Change Management at Brother International Corporation

Ajitha is an IT Leader with depth and breadth of experience, spanning IT Security, Software Engineering, Shared Services, and Digital Experience. With a background in Computer Science and Mathematics, Ajitha is passionate about improving processes and enabling flawless execution. He has deep and varied experience in providing leadership & oversight for strategic assessment, planning & execution of enterprise-wide programs for improving software engineering, security, quality, performance & ecommerce.

Anmol Misra
Director - Infrastructure Security at Autodesk

Anmol is an accomplished leader, author, and security researcher with over 15 years of experience in transforming the security posture of global companies. At Autodesk, he is responsible for cloud and information security. Previously, he held positions at Cisco, EY, and VMware. He is the co-author of two books by leading universities worldwide for application and mobile security and teaches security to students and professionals.

Anuj Puri
Head, Security & Compliance, HCL GSS Sweden at HCL Technologies

Anuj is a Cyber Security Expert with 2 decades of experience and expertise in implementing cyber security measures. His respectable record includes recommending security improvements, evaluating and identifying vulnerabilities and improving overall system efficiencies. Anuj has an impressive capacity to thrive in fast-paced environments while delivering quality results. He is recognised for commitment to customers, motivational team leadership and ability to consistently achieve results.

Acknowledgements

Chiraag Juvekar
Hardware Security Architect at Analog Devices

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Dave Whitelegg
Head of Security Audit and Compliance at Capita

Dave is Head of Security Audit and Compliance at Capita plc, a UK leading provider of digital services, delivering innovative solutions and simplifying the connections between businesses and customers, governments and citizens. Dave has over 20 years of commercial experience in Cyber and Information Security, holding a number of security accreditations including CISSP, Computer Hacking Forensics Investigator, PCI Internal Security Assessor, and ISO27001 lead auditor.

Debraj Chakraborty
Business Development Manager - Network & Security Services at Rockwell Automation

Debraj is a Business Development Professional with 17 years of experience in the networking and Cyber Security domain, helping customers architect the roadmap for a Digital Transformation Journey. He works with industry experts to enable strategic business decisions that are backed by real time data from IACS. With strategic business ideas and a customer-first attitude, he has achieved unprecedented growth in the region.

Christopher Mayo
Assistant Vice President, Security Engineering at PNC Financial Services Group

Fascinated with the possibilities and dangers of an always-connected world, Christopher turned his sights on security, privacy, and data protection in 2010. He has since helped define the security posture of several enterprises and spearheaded development of data protection programs. Christopher works primarily in the financial services field.

David Kosorok
Senior Director, Application and Product Security at DocuSign

David is responsible for DocuSign's application and product security testing program. He has over 25 years experience in software and security testing, and 12 years working specifically in security. Prior to joining DocuSign, David has pioneered application security programs for Align Technologies, SAP Concur, The Church of Jesus Christ of Latter Day Saints, and several start-up companies. David holds a number of professional security certifications

Dmitriy Sokolovskiy
CSO/CISO at Avid

Dmitriy is currently a CISO and CSO at Avid Technology. Previously, he consulted for contractors, public and private companies, and non-profits. He also built and managed a cybersecurity PS team, participating in IR for the largest breaches in US history, later serving as a Cloud Security Architect. Dmitriy advises infosec start-ups, VC & PE firms. He is a SANS Mentor and member of the GIAC Advisory Board.

Acknowledgements

Eric Veum
Director - Product Security at Zynga

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Javier Godinez
Director of Application Security at Teradata

Javier Godinez leads the Product Security team at Teradata. He has been working in the Cloud security space for the last eight years, and has developed a number of applications and patterns for operating in the Cloud securely and at scale. He has previously worked for Intuit, SAIC, and SPAWAR as security architect, red team lead, and software developer.

Jon Winbow
Information Security Director, OnePharma and Consumer Healthcare at GSK

Jon is a Business Information Security Officer with over 18 years of cyber security experience. Jon heads a team of cyber security, risk and compliance experts that interface into two of GSK's largest business areas - pharmaceuticals and consumer healthcare. Previous to this, Jon had global responsibility for operating and evolving GSK's operational security processes, services and technologies for 15 years.

Hank Orofino
Director Cyber Security at Fiserv

Hank has been an IT professional since resigning from the United States Army as Chief Warrant Officer. His IT career of 25 years includes working for technical manufacturing firms, servers, and storage, migrating to the mortgage and banking industry, then technical financial services for global firms. Hank also holds a Bachelor Arts degree and a Masters of Business Administration degree.

Jiang He
Manager, Information Security Risk Management at Sun Life

Jiang is an IT security expert with 12+ years' industry experience across IT risk & controls, security operations, IT governance, telecommunications networks, quantitative modelling, and data mining. Jiang has diverse global experience, and has published a number of research articles in journals, book chapters, and conference proceedings in the field of Technology Management. He holds a Ph.D. in Technology Management and a M.S. in Telecommunications.

Joshua Sorenson
Senior Director, Global Security at Equifax

Joshua C. Sorenson, CISM CISA, is a Security Consultant with Rausch Advisory Services and a thought leader, with over 15 years experience at Fortune 100s including John Deere, Coca-Cola, and Delta Air Lines, in roles ranging from Incident Response to Governance to Security Infrastructure -- most recently he was a Senior Director of Global Security at Equifax helping with post-breach recovery efforts.

Acknowledgements

Karl Mozurkewich
Principal Architect / Program Director, Global Enterprise Architecture at Utropicmedia / OpenText

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Mathieu Ahlstrom
Digital Workplace Solution Manager at Inter IKEA Systems

Mathieu Ahlstrom has a track record of applying business insight to enterprise technology topics, with a focus on digital workplace questions. Most recently he has been working in the identity and access management practice, balancing the ever-growing challenge of global data privacy compliance and rising expectations from users.

Mete Boz
Head of Cybersecurity at Sogeti

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Laura Lees
Country BISO - Australia/New Zealand at Citi Group

Laura has over 20 years of experience in the technology, security and risk management industries with a focus on financial services. She is the Country Business Information Security Officer for a global Financial Services organisation and is responsible for all Information Security related matters in country. Laura is also the current Vice President for the ISACA Sydney Chapter and the Sydney Co-Chapter lead at AWSN.

Mekonnen Kassa
Director of Cloud Security Engineering at Microsoft

Mekonnen has extensive experience in the technology industry leading software and service engineers teams in the design, development, and implementation of many business transforming technology products and services. Currently, he works for Microsoft, leading a global team of customer experience engineers focused on security products. His team engages with enterprises, governments, and institutions to help use Microsoft Cloud security products and services.

Michal Zdunowski
Information Protection Manager at Japan Tobacco International

For over 10 years Michal has been working in the areas of information security, cloud technologies and identity management. He has gained my experience working with many organisations from the public and private sectors, implementing both technological solutions for data protection and compliance programs related to information protection. Michal has successfully obtained the certification of Certified Information Protection Manager and Certified Cloud Security Professional.

Acknowledgements

Niamh Muldoon
Senior Director of Trust & Security, EMEA at OneLogin

Niamh Vianney Muldoon is an award-winning information security thought leader with extensive expertise in creating and leading global security initiatives across multiple industries. Niamh is OneLogin's DPO and Trust & Security Leader for EMEA. Based in Dublin, Ireland, Niamh heads-up all things trust, security, and privacy for OneLogins EMEA operations. This includes driving sales, engineering and customer service activities across the region.

Ophir Zilbiger
Partner, Global Cybersecurity Leader at BDO Israel

Ophir heads BDO's Global Cybersecurity Practice for BDO International, working with BDO firms and the cybersecurity leadership group to develop and grow BDO's cybersecurity practice around the world. Ophir also heads BDO Israel Cybersecurity Center, helping organisations to manage their cybersecurity risk and build their risk based cyber defense. His IT and cybersecurity experience spans over 25 years, across organisations of various industries.

Renato Cendretti
IT Head of Enterprise Applications Security at Nokia

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Nipun Jaswal
Director - Cyber Security Practice at BDO India

Nipun is the author of 11 cybersecurity Books on Penetration Testing and Forensics. With more than a decade of experience in VAPT, Red Teaming and Vulnerability Research, Nipun is presently the director, cyber security at BDO India. He has authored multiple exploits and tools that can be found on popular security databases and has helped many fortune companies curbing cyberattacks.

Peter Kalmar
Service Manager Security Services
at Allianz Technology

Peter is a team-oriented professional with a diverse background in Windows (involving project and customer services) and IT operations (as a technical consultant and engineer). He has strong experience in business continuity management, crisis and change security, service delivery, technology transformation, cloud infrastructure, network planning, virtualisation and compliance. Peter enjoys traveling, fitness, movies, music and cooking.

Robert Behny
Senior Director, Cyber Strategy and Data
at Verisk Analytics

Robert Behny is Senior Director Cyber Data & Partnerships at Verisk Cyber Solutions, Boston, Massachusetts. Robert has led cyber technical risk organisations responsible for security engineering, operations, and compliance activities over his 17 years in the industry. He holds a Certified Information Systems Security Professional (CISSP) certification and multiple certifications from SANS, CompTIA, and cloud service providers.

Acknowledgements

Rodion Varynskyi
Director, Network Operations at J2 Global

Inspired by the rapidly growing and evolving Information Technologies since he was 10, Rodion achieved his masters degree in Technical Information Security and Classified Data Processing automation in 2012. Rodion made his career journey from Technical Support Rep, continuing as an independent security contractor, before joining SMTP.com. Rodion is now inspired and focused on getting internet business technologies to be a privacy-safe and transparently-secured place.

Shafiek Johnson
Information Security Manager at Capita SA

Shafiek is an experienced and highly analytical professional with 8 years of experience performing I.T Risk Assessments, I.T SOX Audits, PCI-DSS and Information/Cyber Security assessments. Throughout his career, Shafiek has amassed comprehensive experience in I.T security and Governance over various industries, such as: Finance, Telecommunications, Travel & BPO (Business Process Outsourcing).

Stuart Leach
Technical Director - Cyber Consultancy at Grant Thornton

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Selva Mahimaidas
CISO at Houghton Mifflin Harcourt

Selva is a top-performing and competent Chief Information Security Officer with more than 21 years of experience in all phases of Information Security. Selva has a proven track record of handling strategic projects and global engagement management, with an ability to recognise business objectives, foresee the solutions, develop approaches, estimate resources, complete tasks, and assignments on time within a budget and maintain the highest quality.

Shitij Bhatia
Regional Cyber Security Manager at Sanofi

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Thomas Zuliani
Information Security & Data Privacy Director at Pandora

PLACEHOLDER TEXT. Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Acknowledgements

Torben Olsen
CISO at H. Lundbeck A/S

Torben started his career in Information Security in 2003, at Danish Institute for Network Security (DINS), where he split his time between penetration testing and preaching about the new Danish security standard DS-484. In 2004, DINS was acquired, and Torben spread his interests to Risk Management and IT Security Governance. In 2011 he left the role of external consultant and joined the pharmaceutical company Lundbeck.

Vitaly Obyazov, CISSP
System Security Manager / Technical Security Center / IT Security Architecture at JTI

Vitaly is an IT security professional with more than 10 years' experience of working in various roles in diverse industries, like Gas & Oil, GameDev, Aviation and Tobacco. Vitaly's expertise covers fields such as IT Security Architecture, IT Security Risk Management, Endpoint Protection, Data Center Infrastructure Security, Cloud Security and DevSecOps. Vitaly has a Master degree focused on Information Security of Telecommunication Systems.

Sources

1. **Embedding new ways of working post-pandemic, CIPD, 16 September 2020**

2-3. **Key investment priorities to secure your evolving cloud environment, Robert Daniels, Senior manager, security portfolio strategy and propositions, BT, 10 August 2020**

4. **We need to rethink cybersecurity for a post-pandemic world. Here's how, Leonardas Marozas, World Economic Forum blog, 13 August 2020**

5. **Impact of COVID-19 on Cybersecurity, Deloitte, 2021**

6. **Securing the Digital Economy: Reinventing the Internet for Trust, Accenture, 2019**

7. **CCS Insight Senior Leadership IT Investment Survey 2020**

8. **Why has there been an increase in cyber security incidents during COVID-19?, Andy Auld and Jason Smart, PwC UK Cyber Threat Intelligence**

TechPros

TechPros.io is a platform for senior business professionals to participate in thought leadership, specifically on changing industry models which are disrupting the status quo. Keep abreast of new trends and opportunities by contributing to thought leadership sponsored by leading IT brands.

Feature in eBooks and panel discussion videos shared amongst your professional community and learn how your peers are overcoming the same challenges.

TechPros.io

How to get in touch

Connect with our team of global business specialists. Email us at businessroi@bt.com or call 1800 924 929

Offices worldwide
The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to the respective British Telecommunications plc standard conditions of contract. Nothing in this publication forms any part of any contract.

March 2021