Telstra Purple

Putting a spotlight on cyber security

IN ASSOCIATION WITH

ATTACKIQ ZIMPERIUM

varmour COFENSE cyberGRX

Telstra Purple

Putting a spotlight on cyber security

WRITTEN BY
SEAN GALEA-PACE

PRODUCED BY
LEWIS VAUGHAN

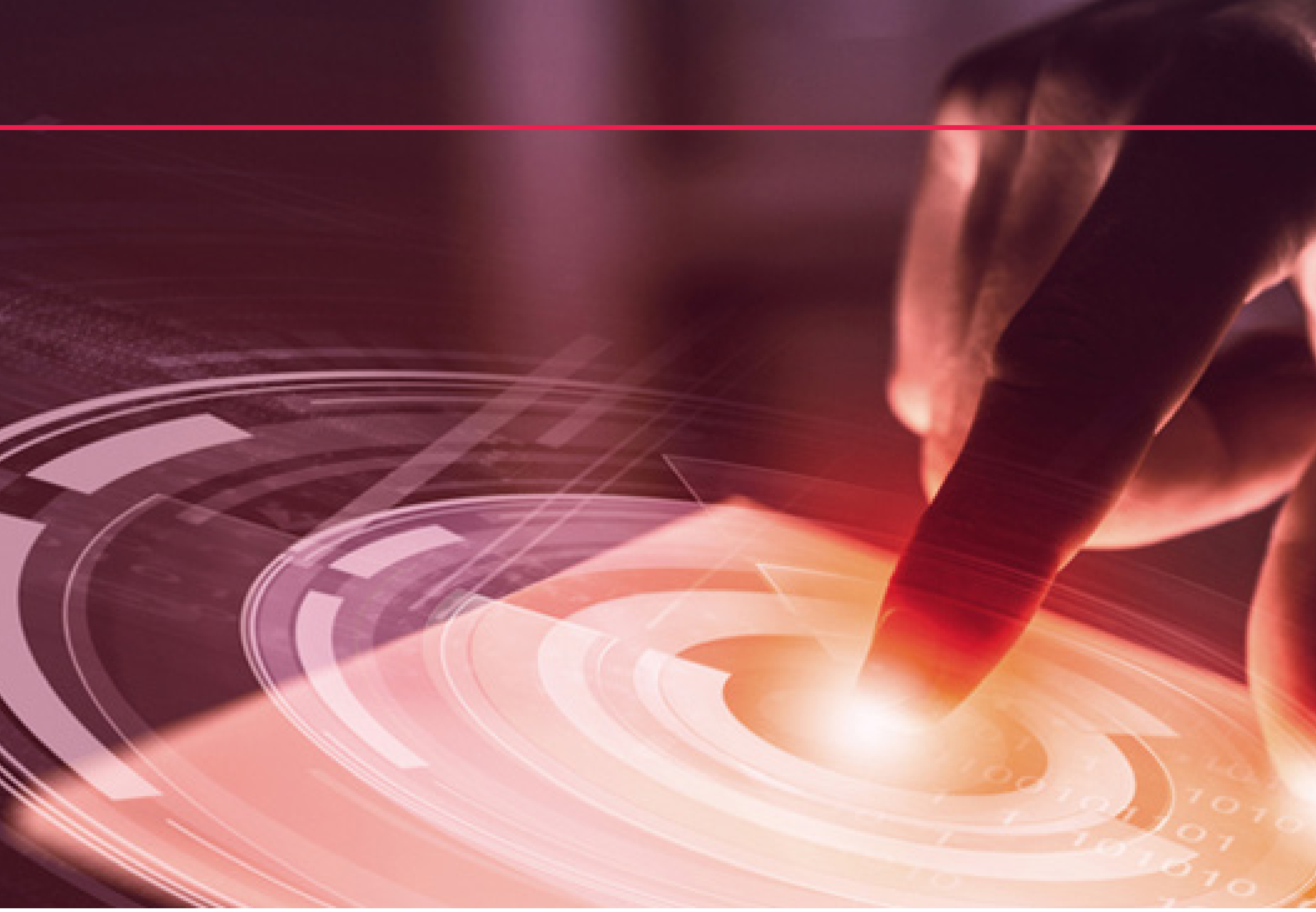
Telstra Purple is a technology services business, comprising of 1,500 specialists in Australia, EMEA and Asia. Bringing together Telstra Enterprise's business technology services capabilities and a number of acquisitions, Telstra Purple is focused on outcome-based, transformative tech solutions.

WHY CYBER RESILIENCE COUNTS TODAY

Geopolitical risks and the impact of COVID-19 have put security technology at the top of every business leader's agenda as the world rapidly responds to the threat. Manoj Bhatt, Head of Cyber Security Advisory and Consulting at Telstra Purple EMEA, has seen first hand the increased focus on risk management and cyber resilience in response to the crisis.

"The coronavirus has demonstrated the importance of cyber resilience as businesses move to remote working whilst ensuring they do so securely," says Bhatt. "Cyber security isn't just a concern for the security or IT department, and those organisations that already have a strong, ingrained security culture that is business wide will weather the storm best."

Username
Password
LOGIN



“The coronavirus has demonstrated the importance of cyber resilience as businesses move to remote working whilst ensuring they do so securely”

—

Manoj Bhatt
Head of Cyber Security Advisory
and Consulting, Telstra Purple EMEA

As business leaders begin to evaluate their technology stacks to understand their efficacy, and consider how well they integrate with the current business while supporting its future needs and goals, security teams must remain one step ahead with answers to potential questions.

Rob Robinson, Director of Security and Network Services at Telstra Purple EMEA, believes that organisations must think of security as a business enabler.

“It goes back to the conversations we’ve been having with CISOs recently. For a security strategy to be successful, all lines of the business – HR, Finance and IT – must stay informed and aligned with its goals," explains Robinson. "CISOs admit to friction within companies, saying they don't think their boards see information security as important a function as they do. It's important that this thinking changes and security leaders offer guidance on how businesses can protect themselves and mitigate risk. Security has to be considered an enabler rather than something that is negatively impacting the business."

"We understand that we're on a journey in the security industry – there's definitely no silver bullet"

—

Rob Robinson
Director of Security and Network Services, Telstra Purple EMEA

CLUBCISO™
Powered by Telstra Purple

Dr Jessica Barker, co-CEO and Socio-Technical Lead of Cygenta, is an evangelist for driving security culture and awareness within organisations. She believes it's essential to operate with an agile approach and remain aware of the latest vulnerabilities to maintain that visibility over potential cyber threats.

"Staying up to date with current attacks is crucial, meaning people in security don't often get very many days off as they need to keep up with the latest news to ensure the greatest level of protection possible," she explains. "However, it is also equally important that we remain vigilant against previous vulnerabilities that we're already aware of, because it could be easy to get distracted by the latest trends or newest vulnerabilities. In many cases, the biggest cyber attacks involve the vulnerabilities that we've been aware of for decades, so it's just as important to remain vigilant against all kinds of attacks."

"Sometimes, the biggest cyber attacks can stem from the vulnerabilities that we've been aware of for decades"

—

Jessica Barker
co-CEO and Socio-Technical Lead, Cygenta and Chair of ClubCISO

Barker is also Chair of ClubCISO, sponsored by Telstra Purple, which is a private members forum for information security leaders, working across public and private sector organisations. More than 350 CISOs are currently registered members. Barker believes there are a number of key advantages to being a member of the organisation.

"We work together to shape the future of the security industry, community and the CISO role," she says. "The idea is to provide a voice to CISOs and offer an environment where they can speak between themselves, and externally, about what the CISO role is and what security looks like moving forwards. It's been great to have a place to build a network of like-minded individuals, share success stories, as well as navigate the challenges in the industry together and work out the best way to overcome those hurdles.

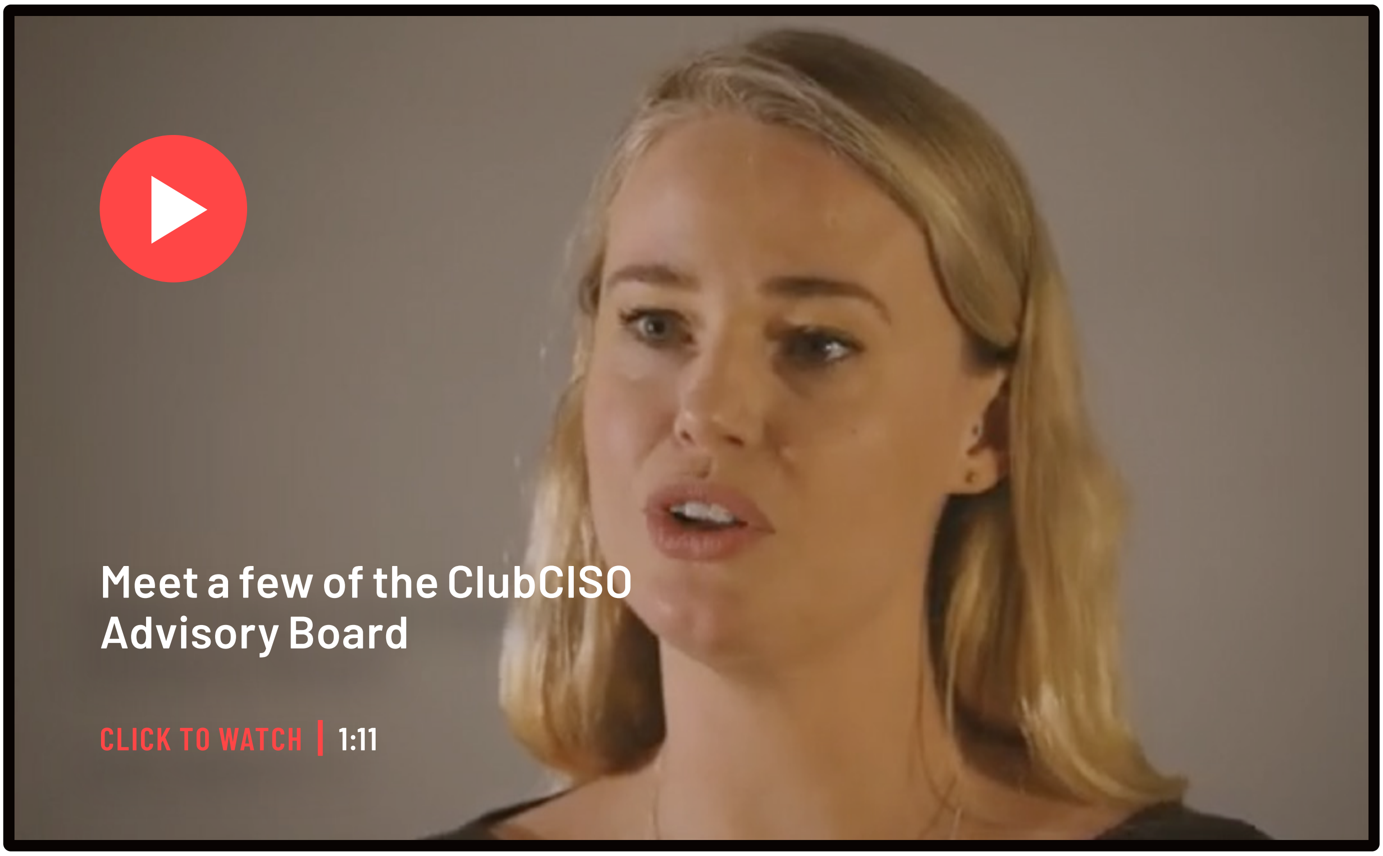
"This year's ClubCISO Information Security Maturity Report reveals some interesting insights on how CISOs are coping with the additional pressures of COVID-19 and other geopolitical risks," adds Barker. "The majority (61%) of CISOs believe that the stress of their job has increased over the past 12 months, yet 70% profess to love their job. I believe one of the most important aspects of a CISO's job today is around cultural change, raising awareness of security threats and figuring out how to embed that cyber security culture within their organisations."

GETTING CYBER SECURITY RIGHT: BEST PRACTICE AND LEARNINGS

Cyber security doesn't sit still, and understanding the latest threats, risks and solutions to these problems is a collective industry effort.

Bhatt also sits on the advisory board of ClubCISO. Explaining the community's benefits he states: "One of the things we really like about ClubCISO is that it's a community of CISOs for CISOs – that's the key thing. It's a peer group to share thought leadership and provide a platform to talk to one another about the latest cyber security threats and issues, and also to share best practices."

Each year, ClubCISO surveys the community in a live vote to get a collective view of the current security landscape and understand the contemporary issues faced by security specialists. The latest ClubCISO Information Security Maturity Report was released in May 2020. This year's live vote, which was held virtually for the first time due to the COVID-19 outbreak, drew over 100 CISO respondents.



Meet a few of the ClubCISO Advisory Board

CLICK TO WATCH | 1:11

> “We are seeing a reassuring shift in security investment and awareness, something which is vital for organisations to remain digitally agile”
>
> —
>
> **Manoj Bhatt**
> Head of Cyber Security Advisory
> and Consulting, Telstra Purple EMEA

“One surprising finding from this year’s report is that there isn’t as much maturity around the cloud as expected,” states Robinson. “We have asked that same question five years in a row, expecting the percentage to increase considerably each year. However, it has remained the same.”

Robinson postulates that this stems from a shortage of skill sets. Another related conversation in this space revolves around how to encourage more diversity in security – sparking an interesting debate around what security teams can do to be more inclusive and

EXECUTIVE PROFILE:

Rob Robinson

Title: Director of Security and Network Services at Telstra Purple EMEA

Rob Robinson is the Director of Security and Network Services at Telstra Purple in EMEA and has over 15 years of experience in Business and Technology Advisory Services, working within consultancies, integrators and telecommunications companies. Prior to Telstra Purple, Rob joined Company85 through the acquisition of DVS Services in 2015, where he was the owner and Managing Director. As an advisor to CISOs and CIOs, Rob has first-hand experience of helping teams assess their position, build their strategy and deliver successful programmes. Working with his team in the UK and in his capacity of Security domain lead for Telstra Purple globally, Rob delivers programmes of change across multiple industry verticals.

build up capabilities. To resolve the issue for future generations, Robinson believes it's important to start talking about security apprenticeships early, and begin to raise the importance of it in schools now. "It's vital to talk about the importance of security and feed that interest into the security industry at a time where we increasingly need that help and capability," he says.

The coronavirus pandemic has caused disruption in industries worldwide. Uncontrollable circumstances such as these highlight the importance of adopting a 'future state' mindset, reassessing business needs now and in the future, and evaluating what kinds of technologies and implementations can support these. The priority in the current environment is supporting home working and guarding against cyber threats.

Bhatt sums up the current situation and issues a warning: "We're certainly seeing a big drive from a number of vendors talking about how their security products are going to be 'the silver bullet', but it's impossible to determine a solution without a proper assessment and understanding of business needs first.

"You must first understand what already exists within your organisation, and what the current technology set up is, before you can consider what the best technologies for the job are. If you bring this thinking together, it makes you more resilient against threats, whether that be COVID-19 or an out-of-the-blue cyber attack. It's important to join the dots and take a holistic perspective."

THE POWER AND THE THREAT OF EMERGING TECHNOLOGIES

As emerging technologies such as machine learning (ML) and

automation become increasingly sophisticated, so do those with malicious intent. Businesses must be prepared to keep pace with the threat environment to remain secure.

“The world’s changing,” states Robinson. “We’re not in a traditional bubble where security is at the perimeter and everything’s protected centrally – there’s a much wider attack surface. There’s a lot of information sitting outside of non-traditional environments and you have to apply technology and modern approaches such as ML and automation to that,” he affirms.

“It’s important that we apply these technologies in a way that’s appropriate, as well as maintain an accurate understanding of how we address and manage security incidents, otherwise businesses will not be in a position to respond and protect.”

Whilst cloud is not exactly an emerging technology, many businesses are still at the nascent stage of their cloud

journey. Bhatt has observed that businesses are split into three different camps when it comes to their cloud security strategies.

The first camp thinks about cloud, but has not embarked on the journey because they haven't considered where it might take them. The challenge is in identifying what cloud will achieve for the business, and how much can be saved by implementing it.

In the second camp are businesses that have implemented cloud but are not recognising the benefits it is delivering. These are typically organisations that have not set out a clear path or taken an objective-driven approach to their cloud strategy.

In the final camp sit the businesses with cloud expertise that focus on cloud enhancement. This is where a company has moved to the cloud and is now looking to enhance it with approaches such as containerisation. This marks the start of the next stage of the journey, where

Introducing a navigation system for your hybrid cloud.

vArmour Helps Security Teams Navigate Operational Risk

The relentless pace of digital business means more risk. As applications proliferate across clouds, so too do the relationships between them—exponentially. Of the hundreds of thousands of relationships in and across your clouds, do you know which of those might be malicious? Which are connected to a critical asset? vArmour leverages the technology you already own to measure, model, and control your risk.

Start your journey at vArmour.com.

varmour

Relationships Matter

technologies such as automation and robotics become increasingly influential in the business.

With the pace of technology adoption showing no sign of letting up, it's vital that businesses and their employees practise good cyber hygiene at their workplaces and homes.

"Security is a continuous journey that must be grounded in what the business is trying to achieve," says Robinson. "Business leaders and their security advisors must assess the environment the business operates in, understanding the risk landscape, the threat profile and how you place people, processes and technology around security to address these evolving needs. And finally, cyber security must align with all business functions to ensure there are no weak links."

Telstra Purple

CURITY
BREACH
Details

CLUBCISO INFORMATION SECURITY MATURITY REPORT 2020

Top three areas where CISOs have driven measurable improvements over the last 12 months:

- Security awareness and training
- Risk assessment and management
- Building the security team

Top three hot topics on the CISO radar:

- Security culture
- Cyber resilience
- Cloud security

The top three initiatives CISOs are using to foster a better security culture:

- Security champions
- Proactive "report it" no blame policies
- Education around the value of data

To check out the latest ClubCISO Information Maturity Security reports, click here

EXECUTIVE PROFILE:

Manoj Bhatt

Title: Head of Cyber Security Advisory and Consulting at Telstra Purple EMEA

Manoj leads Telstra Purple's cyber security advisory and consulting capabilities for EMEA, working with a wide range of customers across numerous sectors building and running their cyber security services. Manoj is a passionate cyber security professional focused on embedding cyber security into the digital agenda and on the user and customer experience aspects of cyber security. Manoj sits on the advisory board for ClubCISO to share security innovations, best practice and thought leadership across the industry.

VENTURES

Telstra Ventures is a strategic growth investor passionate about scaling great products and leaders. An independent venture capital firm backed by Telstra and HarbourVest - one of the world's largest private equity funds - it provides venture capital investment via a 'Strategic Growth Investment' approach. This offers entrepreneurs access to the investment itself and reduces the time to reach global scale.

In almost a decade, Telstra Ventures has invested over US$350mn in 60+ companies.

Marcus Bartram is a founding Partner at Telstra Ventures and leads the security portfolio for ventures. His main role is investing in new security startups, and then helping them scale to become successful large companies.

Telstra Ventures invests heavily in security ventures and is continuously seeking the best-in-breed security innovators globally. With expertise in picking cyber security companies to invest in and helping them scale, Bartram believes it's critical to pick a sector that you have a clear understanding about.

"The best way you can understand a particular area is to go out and talk to as many people in that sector as you can, be it entrepreneurs, customers or vendors," says Bartram. "Figure out who the best companies are, what they're building, who the customers are and what problems they're trying to solve. This will enable you to build a really rich knowledge base that informs where you invest."

Telstra Ventures has an extensive portfolio of companies in the cyber security space such as Anomali, Auth0, CyberGRX, AttackIQ, Cofense, CrowdStrike, Varmour and Zimperium.

Bartram notes there are several key areas to scrutinise before investing in a cyber security startup: "It's important that I understand who's the team, what pain point they are solving and how many customers do we think have that problem, what product have they built, and what trends are driving that market. We also consider if the deal makes sense financially. You've got to find the right combination of an amazing team, product and market that has the potential to allow the company to scale."

CROWDSTRIKE

"This is a threat intelligence company in California. We invested in (the founders) George and Dmitri, because they are very experienced security guys who were redoing protection on the endpoint and disrupting the existing vendors, detecting threats that other technology just couldn't see.

"Telstra was a very early customer. Crowdstrike is now the highest-rated vendor by Gartner in Endpoint Detection Response Solutions. It proved to be a really great investment for us because we felt that they had the best technology, the team was amazing and customers were clamouring for a better solution."

ATTACKIQ

"This company provides continuous validation of enterprise security programmes. They're trying to help CISOs answer the question: 'How secure am I?'. They do that by deploying a platform that effectively tests all the security tools, people and processes on a continuous basis.

"AttackIQ can test all the control points in your environment, be that cloud, endpoint, network protection or controls. This is done by simulating attacks against those controls, and it can become a risk tool for CISOs as they can look at their environment in real time and measure the risks they face."

CyberGRX

“This is a risk mitigation specialist focused on helping customers understand and manage cyber security risk from their supplier base. The company has built a data exchange which drives massive efficiency in how customers and suppliers collect and share information about their cyber controls.

“It is an incredibly important part of the security sector that affects every organisation globally in the same way. Regulatory drivers, the explosion in the number of suppliers companies use, and companies needing to protect themselves from threats that come from these suppliers make CyberGRX a great company to be a part of.”

COFENSE

“Cofence was set up to counter phishing - still the most common, never-ending problem facing the security industry. During the COVID-19 pandemic, phishing is being massively exploited by criminals.

“The founders, Rohyt and Arron, started out by building technology to help employees recognise and report phishing emails, to raise the bar and stop people from opening links and attachments they shouldn’t. They have evolved from this to create a sophisticated platform that now integrates and shares data with their customers from tens of millions of data points on all the phishing threats they see, helping to protect customers from phishing attacks.”

vARMOUR

“This is a company that lets you visualise and understand all of the traffic and application flows across the environment, particularly in a multi-cloud or hybrid cloud world. That visualisation allows you to figure out who’s talking to whom and whether those conversations are OK. From that you can design the security controls to implement.

“The platform integrates into all of the native security controls in

AWS, Azure, Google Cloud or VMware to provide visibility into what's going on and then be able to protect the customer. Customers are using this for cloud migration as much as they are using it for security controls."

With the future in mind, Bartram affirms it's essential to continue to seek value in innovative companies globally.

"We must continue to try and invest in these leading companies, because it is good for us, the entrepreneurs and customers in the long term. Telstra Ventures wants to invest in innovative startups in security, cloud, enterprise and consumer platforms, insurtech, healthtech and many other fields, helping those companies scale through Telstra and other relationships. We think and work incredibly hard to find the best companies, and assess how well they will perform. We remain passionate about finding the best entrepreneurs with a passion to build amazing products, which solve real problems in the world today and into the future."

EXECUTIVE PROFILE:

Marcus Bartram

Title: Partner at Telstra Ventures

Marcus is a founder and General Partner of Telstra Ventures. Prior to this he held various executive and senior roles in Telstra, Citigroup, nscglobal and Honeywell in Australia and the UK. Marcus invests in disruptive enterprise software, telecoms and cyber security entrepreneurs that are starting to scale their company. Investments made to date include Anomali, AttackIQ, Auth0, Cohere Technologies, Cofense, Crowdstrike, Corvus Insurance, CyberGRX, Elastica (ACQ:BlueCoat), Headspin, ipSCAPE, Matrixx Software, Dimmi (ACQ:TripAdvisor), vArmour and Zimperium. Marcus received an MBA from the University of Oxford and a Bachelor of Engineering from the University of Adelaide, South Australia.

Telstra
Purple

BLUE FIN BUILDING
110 SOUTHWARK STREET
LONDON SE1 0TA

www.telstrapurple.co.uk

POWERED BY
BizClik
MEDIA