BROADGATE

Cybersecurity Insights *Report* 2023

Introduction

Welcome to Broadgate's inaugural cybersecurity insights report, a deep-dive into the trends, challenges and changes that the industry expects to face in 2023. We developed this report with the thoughts and insights of five unique thought leaders operating in the space today.

Amidst the meteoric rise of startups, the relentless evolution of technology and the worldwide transition into the post-COVID era, data concerns in the cybersecurity market have grown exponentially.

From paradoxical talent shortages to the rapid emergence of new-age tech, in an industry governed by constant change, the world must learn to prioritize the value of cybersecurity talent.

Contents

Bios

Andrew *Obadiaru*

Chief Information Security Officer

Andrew Obadiaru is the Chief Information Security Officer at Cobalt, which provides a Pentest as a Service (PtaaS) platform that is modernizing the traditional, static penetration testing model. At Cobalt, Andrew is responsible for maintaining the confidentiality, integrity, and availability of Cobalt's systems and data. Prior to joining Cobalt, Andrew was the Head of Information Security for BBVA USA Corporate Investment banking, where he oversaw the creation and execution of Cyber Security Strategy.

Andrew has 20+ years in the security and technology space, with a history of managing and mitigating risk across changing technologies, software, and diverse platforms.

Malia *Mason*

Manager of Security Operations and Engineering for Corvus Insurance, Co-chair of the Tech for Good Committee at AnitaB and Co-founder and President at CyberDEI.

Malia Mason is a United States Navy veteran, an ally, and advocate for equal representation. She is an established cybersecurity leader and frequent conference speaker. She is the President and Co-Founder of CyberDEI as well as Co-Chair of the Technology Committee for AnitaB.org. Malia had the distinct honor to be a community organizer for AnitaB.org's first-ever Women of Color in Tech conference in Los Angeles. She serves on the advisory board for 3 local community colleges, and mentors girls in middle school and high school at CyberTech Girls and GenCyber Girls. She frequently mentors veterans and mil-spouses and collaborates with various veterans' nonprofits.

Cobalt

cyberDEI
Diversity, Equity & Inclusion

CORVUS

ANITA B.ORG

Jacob *Simmonds*

Team Leader

A Recruiting and Staffing professional with 8 years' experience, Jacob Simmonds leads Broadgate's West Coast Cybersecurity division. With a diversity-focused approach to building robust teams, Jacob is equipped to help businesses everywhere deal with a perpetually evolving threat landscape.

Jacob specializes in Cybersecurity (Cloud, AppSec, Offensive Security & SecOps/DevSecOps), Information Security (GRC, Data Protection) and Executive Search (C-suite to BOD).

Alon *Nachmany*

CISO and Principal Consultant

Twenty years in the cyber security space may seem like a long time, but to Alon Nachmany, it's only the beginning. After earning an MBA from Tel Aviv University, Nachmany hit the ground running, leaping headlong into the security space and serving as a CISO and an IT & Security executive to a number of financial institutions. He prides himself not only on having helped to protect others' finances, but on leading the charge as financial firms became increasingly reliant on digital technology.

Finance isn't Nachmany's only passion, however. He has also lent his expertise to a number of government agencies, protecting our nation's most precious, proprietary, and vulnerable assets. Nachmany's commitment to innovation and excellence in the cyber security space has afforded him the opportunity to protect organizations like National Securities Corporation (now B. Riley Financial), WeWork, Forex Capital (now Jefferies Financial), AppViewX, and Bromium (now HP). He intends to pursue his passion of preventing digital crime while implementing effective cost-saving measures for the foreseeable future. Alon was listed on Top Cyber News Magazine's 40 under 40 for 2023 Global Cyber Security.

BROADGATE®

AZEN CONSULTING

Kiran *Sharma*

Cyber Secruity and Data Privacy Enthusiast

Cyber Security and Data Privacy Enthusiast with 15+ years of experience leading essential Security and Privacy programs and delivering projects, processes, tools, and standards that ensure cyber resilience and global compliance. Ability to optimize enterprise cybersecurity and privacy for financial services, Fintech, and Healthcare Industry.

He has the expertise in translating evolving industry risks and a myriad of privacy regulations into ambitious technology around a proactive defense by continually sharpening the company's security and privacy maturity and aligning solutions with well-known industry frameworks.

Talent Shortages: *A Far-Flung Fallacy?*

Mass Layoffs

Headlines are awash with talk of talent shortages, and while the glaring chasm between candidate and career opportunity is hard to ignore, it hasn't prevented businesses from firing their experienced cybersecurity staff.

The mass layoff trend sprang into life at the start of the pandemic, but it's since stuck around (much to the dismay of those in the security space). As a result, unrest is building throughout much of the already exhausted cybersecurity community.

While many of the recently laid-off employees are quickly getting scooped up by other companies, it's still a worrying trend that sees the individual's get put at risk, having been left to think 'are we going to be next?'

Laying off staff amid complaints about talent shortages is almost as contradictory as it sounds, but there's plenty of complex factors driving this decision, not least of all a misunderstanding of role requirements, a tumultuous economic landscape, pressure from the conflict in Ukraine, and the rise of nation state-backed hacking groups.

When the shape of the economy necessitates radical cuts, it's often the cybersecurity professionals that go first.

Misunderstanding the Requirements

At the beginning of COVID, it wasn't out of the ordinary to find a job ad requesting 15 years of Zoom experience – a platform that's only been in existence for 11 years.

This disconnect between the role requirements and the way that those requirements are being advertised or perceived is indicative of poor communication. Entry level cybersecurity jobs that demand between 7 to 10 years of experience are not entry level jobs at all.

Moreover, failing to sufficiently advertise the role actively prevents the top talent from ever applying in the first place. This disproportionately affects women too, in an industry that already suffers from a representation problem. An example of this can be seen through the lens of the job ad criteria – *Some research* has claimed that women tend to only apply to a job if they meet 100% of the criteria, compared to men, who will apply if they manage to meet only 60%.

Diversity-led hiring methodologies are needed to ensure that access to the available talent pool is as wide as possible.

One way to get around this, is to give cybersecurity a seat at the executive table, letting it in to the wider business conversation. Until this happens, plenty of organizations will continue to see their security as a cost center, rather than a business partner.

There's a distinct lack of companies trying to tap into the talent that they already have, and when this is combined with a lack of role understanding, perpetuated by the myth that cybersecurity functions are solely a cost center, makes the recruitment process incredibly difficult to approach for many.

A *Lack* of Training & Learning

‘I wouldn’t presume to say the talent shortage is a fallacy, given the amount of talent in the market,’ notes Jacob Simmonds, ‘but there is a massive gap in training and learning.’

This helps to explain where exactly the talent gap is, and what it means beyond the buzzword that it’s turned out to be – the talent is out there, it’s partly a question of knowing how to find people, maximizing the value of existing talent, and providing the right kind of training to ensure that they have the competency to take on more technical roles.

It’s not a blanket absence of training however, as for many, there have been great strides made in the training and learning aspect of employee investment.

Changing *Perceptions* of the Industry

Visibility

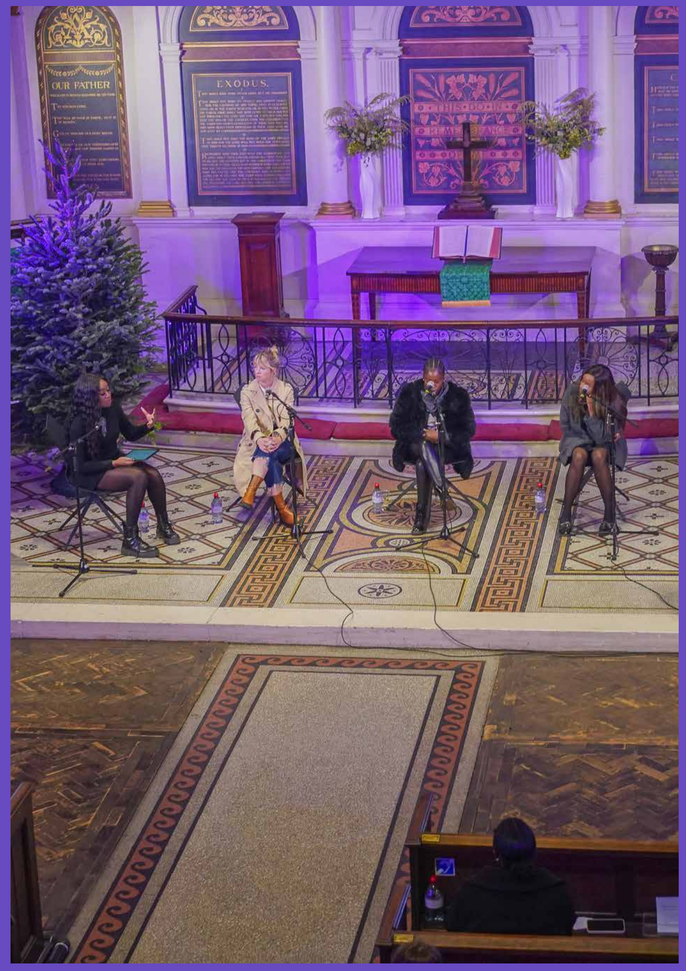
When stigma distorts the outside perception of the industry, barriers start to emerge, and the doors to a lucrative and rewarding career become firmly locked (or completely invisible).

Opening these opportunities and making cybersecurity careers viable for everyone means advocating for visible representation in the space.

In a digital world that most of the population interact with in at least some capacity, cybersecurity is a topic that effectively concerns everyone, therefore the entryway into the space should be visible to all. Demystifying the industry by showcasing the diverse leadership that does exist already can normalize cybersecurity as a career, acting as a catalyst to draw it out of the shadows and populate the industry with new talent.

The lack of diverse talent represents a perpetual cycle that seeks to widen the digital skills gap: A lack of industry diversity is not enticing for a diverse generation of candidates.

Gen Z, the first generation of digital natives, are the most diverse and populous group of individuals on the planet, and *the majority of them have an inclusive-first mindset.*



Normalising Cybersecurity as a Career

Cybersecurity professionals aren't all the eerie, ethereal individuals that much of popular media insists they are.

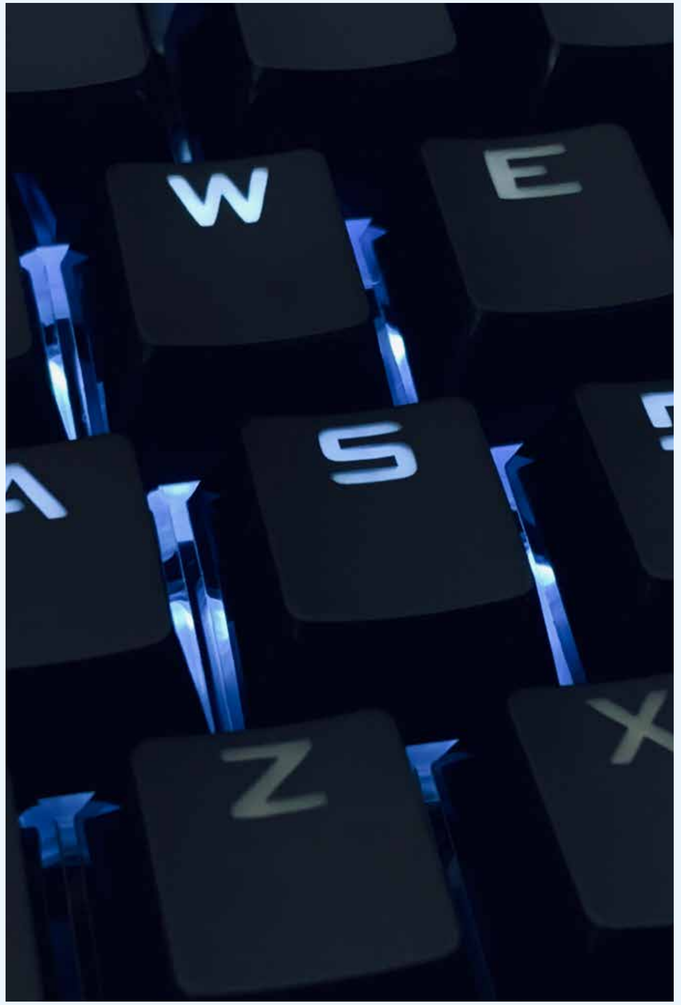
The onus falls on the industry to be transparent about their work, or perhaps more precisely, what that work looks like – another aspect of the field that's traditionally been hindered by poor communication.

An IT degree isn't necessarily essential in understanding the very real, tangible threat of cybercrime and what it represents, yet many stray from learning more because of the heavy association with technical language.

Terminology changes (threat actor instead of hacker for example) have a role to play in making this field more accessible and preventing a strenuous relationship between the security professionals and the
business leaders.

The Ever-*Present* Threat of Breaches

Breach *Fatigue*



While breaches are still the major concern of the cybersecurity space, for some, having data stolen is almost expected. The attitude of, 'threats have crossed the threshold already, my data is out there, what's the point in caring?' Is an attitude shared by many weary executives.

Breaches are now so common, that some businesses simply view them as part of the general operating costs. Absorbing the costs associated with a successful data breach is not a luxury that many have, nor is it a moral option, even if they could.

Important questions about accountability must be raised in this space. *Who takes the blame?* The *FTC recently targeted Drizly's CEO*, James Cory Rellas, with fines for security failures that exposed the data of 2.5 million customers.

The move shifts focus to the individual, in what *the Washington Post labelled as a 'rare' order*, perhaps signifying the beginning of a new approach to breach crackdowns.

It's not as if the majority of these threat actors are professionals either. In many cases, they've been known to inadvertently encrypt the ransomware itself, meaning there's no way to even contact them or read the ransom note in the first place.

A *Low* Bar to Entry

The rate in which adversarial factors are driving the market is astonishing, and the rise of ransomware as a type of illicit industry is largely to blame.

The tools and programs required to carry out a successful cyberattack are easier to get hold of than ever before. Technically, all you need is access to the dark web and a spare $20 in the bank.

Unfortunately, those who go down this route stand to gain a great deal from investing not very much at all.

There's been *reports* of DDoS 'attack packs' being sold for as little as $5, and when combined with some technical knowledge, this becomes a sinister danger. With a lower barrier to entry, the field opens to a greater number of trolls with the need to disrupt – *Uber was breached by an 18-year-old back in September*, who did little more than torment the company's Slack channels once he gained access.

It's not as if the majority of these threat actors are professionals either. In many cases, they've been known to inadvertently encrypt the ransomware itself, meaning there's no way to even contact them or read the ransom note in the first place.

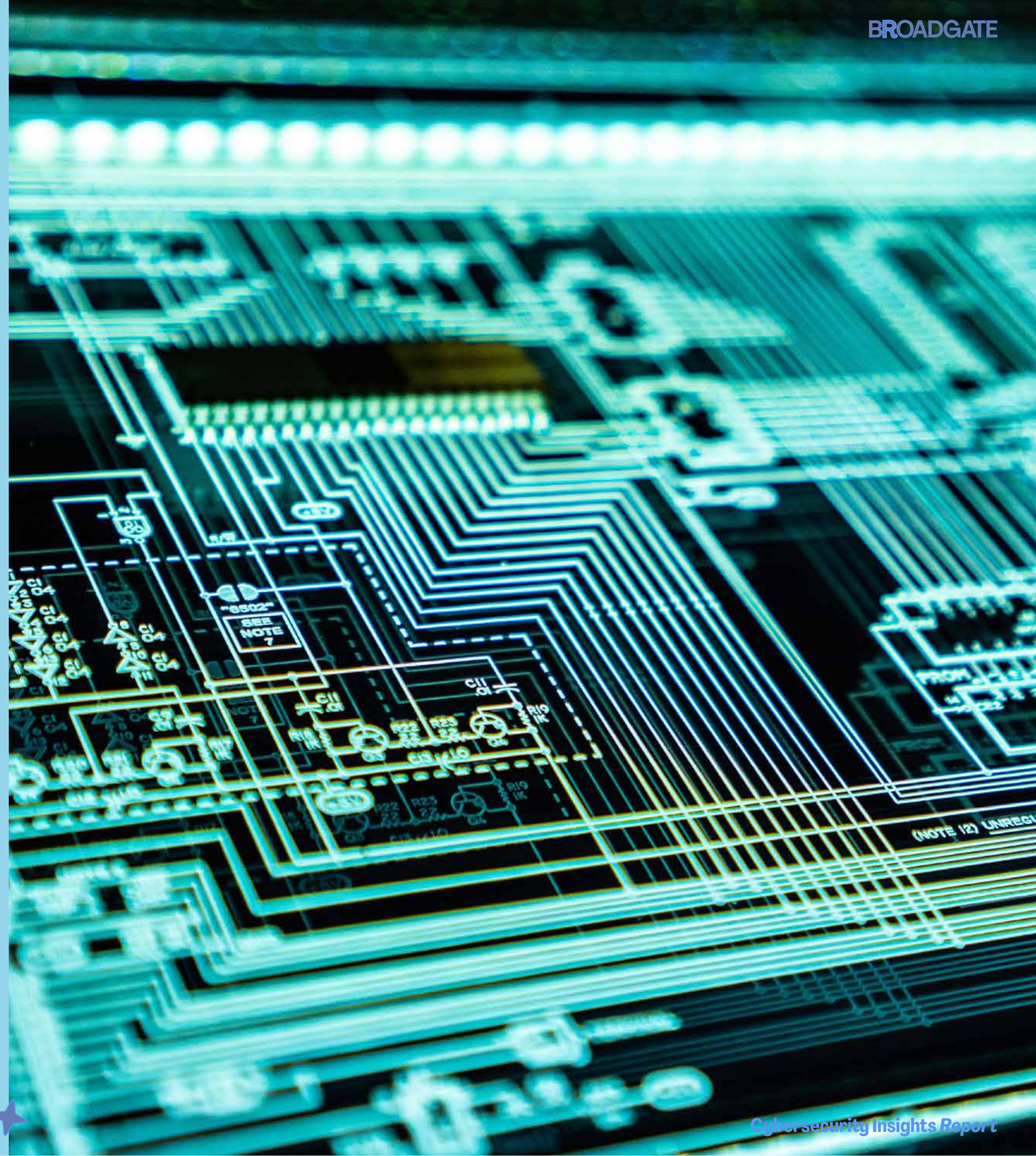
New Tech, *Old Threats*

‘The realm of AR and VR was the wild west before regulations were introduced.’ Says Malia Mason, ‘Where the technology is way ahead of the regulations and government, it’s a catch-up game. And it just sucks.’

Leading-edge tech tends to prove troublesome in the world of policy and regulation. It’s tough to write guidelines and compliancy laws for a product that’s not yet fully explored.

The threats are more or less the same too, they just have a different face, quite literally – Deepfake technology is hauntingly advanced, and it’s being used to bypass MFA and trick people into believing they’re talking to their colleagues.

Deepfake threat actors have been looming on the horizon for a while, but now that they’re here and ready to cause havoc, where are all the solutions? The recent deepfake of Ukrainian president Vladimir Zelensky ordering his soldiers to surrender is a stark reminder of the devasting potential this tech has, or as *CNN reported:* ‘a warning for corporate America.’



A Tumultuous World

The war in Ukraine continues to represent many extreme challenges in the world of cybersecurity, threatening the wellbeing of both critical infrastructures and private organizations everywhere.

CISA released *a report* earlier this year that documented Russian state-sponsored cyberthreats, serving as a warning for organizations of all shapes and sizes. Similarly, what is a perhaps a correlation as (opposed to a direct connection) to the Ukraine conflict, supply chain management has emerged as a key driver for market growth.

Outside threats are poised to continue making misery, and many of them are backed by nation states. *The New Yorker reported* on the rise of North Korea's 'Hacking Army' in 2021, a rise that purportedly contributes to a huge amount of revenue for the Kim dynasty.

These elaborate and devasting attacks aren't new - the North Korean group known as Lazarus is suspected of being behind some of the most high-profile digital thefts of the last decade, including an *$81 million digital heist from the bank of Bangladesh back in 2016*. Organizations must understand that they are a target, and outside threats are going to cost them. To understand the 'why' is the first step toward a more secure future.

Understanding *People*

Cultivating a cultural awareness and fostering a better understanding the human motivation is a vital part of cybersecurity. In a global-facing (or at least, globally susceptible) market, advocating for diversity of thought is critical in both understanding differing viewpoints, and finding new security solutions.

'Cybersecurity is 100% all about humans.' Says Alon Nachmany, 'anyone who tells you it's all about tech, doesn't know what they're doing.'

Combatting the greatest issues in cybersecurity is about predicting human nature, anticipating user behavior and getting inside the mind of the threat actor, and this can only be done by fostering an understanding of the external pressures facing the population on both a localized *and* a global scale.

The *Mysteries* of a Remote World

Unexplored *Opportunity*

It seems like nearly every company utilizes a public-facing web application, acting as a potential breach point that needs protecting.

Companies are realizing that protecting themselves, their employees and their clients in the remote space is crucial to success in today's hybrid climate, yet the majority of this space is still unexplored.

Emergent trends and technologies (the zero-trust model being a good example) are shaping the future of cybersecurity, and as usual, it's left many racing to understand the number of opportunities available.

The Ecommerce *Hotspot*

The world's Ecommerce platforms are driving tremendous market growth for a host of reasons, one being the increasing need to protect assets in the space.

Ecommerce will likely always be a hotspot for cybercriminals, and as the threat actors become more sophisticated, so too must the solutions used to stop them in their tracks.

As the Ecommerce space grows, it's forced more organizations to implement additional measures in order to protect not just their assets, but the entirety of the organization. This upward trend looks set to continue too. The more incidents, the greater the need to search for solutions outside of the normal parameters.

Hybrid Working's **Biggest *Challenge***

The global connectivity and ease of remote access promised by hybrid working are game-changers when it's done right, but as a concept, it's still very much in its infancy.

Cybersecurity is no stranger to remote working, but when the rest of the world went digital at the start of the COVID pandemic, the landscape was changed forever.

More employees online represent a much greater potential for data breaches, begging the question: 'How do you build a process that will secure your environment when folks are accessing it from wherever in the world they're working from?'

VPNs have proven effective in the past, a move to a zero-trust model could provide fill in the security gaps that a traditional approach leaves wide open.

Future *Predictions*

Adversarial factors will continue to drive the market in the never-ending back and forth that is cybersecurity. As we stand on the precipice of great change, companies that recognize the inherent value of cybersecurity as a foundation of the business, and not as another cost center, will be the ones to retain their competitive edge.

Here's what the experts had to say:

Malia *Mason*

"Disinformation and deep fakes are the future that we're not addressing in security. We've already seen three or five major security attacks using deep fakes, and we're going to continue to see folks get fooled."

Alon *Nachmany*

I think we're going to see a shift in spending from what's cool, and intuitive to what works. People are going to concentrate more on that, and there's going to be more room for automation as a way to cut costs.

Kiran *Sharma*

You need cybersecurity experts, which means having some sort of training mechanism internally. You don't need to have a cybersecurity expert, per se, but having cybersecurity champions in each team would definitely help. Creating that cybersecurity awareness in the organization is always the key.

Andrew *Obadiaru*

I am still a firm believer that the human factor is the key to true security and protection. If people take their security awareness seriously, and they understand the basic parameters of what's expected of them, it becomes very difficult to compromise.

Jacob *Simmonds*

I hope that companies will start to understand the market a little bit better, and start to value security talent in the same way that perhaps a superstar like a DevOps engineer would be remunerated.

Contact & *Connect* with us

Sabrina Battiston
Business Manager
+1 323 244 2345
sabrina@trustinsoda.com

Jacob Simmonds
Team Leader
+1 310 256 2677
jacob.simmonds@broadgatesearch.com

Tovah Jackson
Associate
+1 213 292 5886
tovah@trustinsoda.com

Steven Vo
Associate
+1 323 244 2349
steven.vo@trustinsoda.com

Nicola Munson
Associate
+1 424 217 1997
nicola@trustinsoda.com

Youssef Bayrem
Trainee
+1 213 823 4900
youssef.b@trustinsoda.com

BROADGATE

London
+44 203 762 2010

**52 Bedford Row,
4th Floor,
Holborn,
London
WC1R 4LR**

Manchester
+44 161 694 6286

**1 ST Peters
Square,
Manchester
M2 3AE**

Los Angeles
+1 657-276-4702

**WeWork - 10th
Floor
222 Pacific Coast
Hwy
El Segundo, CA
90245**

Boston
+1 617-849-8982

**77 Sleeper
Street,
Boston,
02210**

Zug
+44 41 562 50 59

**Baarerstrasse
135,
6300 Zug,
Switzerland**

Dublin
+353 1905 8602

**WeWork
Charlemont
Exchange,
42 Charlemont
Street,
Dublin**

Broadgatestaffing.com

SIA STAFFING INDUSTRY ANALYSTS 2022 Best Staffing Firms to Work For in the UK & Ireland

TIARA RECRUITMENT AWARDS WINNER THE WORKWELL DIVERSITY, EQUITY & INCLUSION AWARD

WORLD CLASS TO WORK FOR 2022

TIARA RECRUITMENT AWARDS WINNER THE TWENTY20 CAPITAL BEST RECRUITMENT COMPANY TO WORK FOR (£20m-£50m)

INVESTORS IN PEOPLE® We invest in people Platinum