

Security

ADVISOR

MIDDLE EAST

- * SPECIAL REPORT: PROTIVITI
- * WOMEN IN TECH

BATTLE READY

ROSS BREWER, CHIEF REVENUE OFFICER AT SIMSPACE, TELLS ANITA JOSEPH HOW THE COMPANY HELPS WITH BUSINESSES WITH CONTINUOUS SECURITY IMPROVEMENTS AND DELIVERS QUANTITATIVE AND ACTIONABLE INSIGHTS INTO HOW ORGANISATIONS CAN PROTECT CRITICAL ASSETS AGAINST CYBER THREATS.

Observability for every journey.

Value wherever you start.

- » Over 300,000 customers in 190 countries, from small and medium-sized businesses to Fortune 500® companies
- » 499 of the Fortune 500 are customers
- » 50+ IT management products

solarwinds.com

Join us at GISEC Booth A.50



NETWORK
MANAGEMENT



SYSTEMS
MANAGEMENT



DATABASE
MANAGEMENT



IT SERVICE
MANAGEMENT



IT SECURITY



APPLICATION
MANAGEMENT

CONTENTS



6 News updates from the cybersecurity world and beyond.

10 Harish Chib, Vice President MEA, Sophos, on the threat landscape, ransomware, CryptoRom scams and XDR

20 Werno Gevers, Regional Manager, Mimecast Middle East, on how the company helps organisations implement a complete, holistic strategy to reduce Business email Compromise risk.

30 Resecurity on how Digital Smoke has demonstrated how bad actors leverage cross-border payments and jurisdictions to complicate further investigation and identification of their victims.



Be **data** ready.

Commvault is a worldwide leader in delivering data readiness. Our intelligent data management solutions work on-prem and in the cloud, allowing you to store, protect, optimize, and use your data. Always.

commvault.com

EDITOR'S NOTE



Talk to us:
E-mail:
anita.joseph@
cpimediagroup.com

Anita Joseph
Editor

FACING THE ENEMY

Security is all about facing the enemy, very often, head-on. This issue of your favourite magazine is all about getting ready for battle with the enemy. Let's face it, the adversaries have stepped up their game and now its up to the defendants to match up to it. Organisations and the people who run them are slowly perceiving cybersecurity to be a slightly different ball game than information security. As global businesses grapple with increasingly complicated cyber threats and aim to keep their enterprises safe from malware, hackers and other forms of threats, their understanding of this domain is getting richer every day.

However, cybersecurity management cannot happen in isolation – appointing one security officer to handle everything in cybersecurity is not going to make an organisation efficient or secure. There needs to be a specialised team whose sole task should be to manage the entire paradigm of cybersecurity for a business.

Our cover story this month is about how SimSpace helps organisations answer several sophisticated complex questions they can answer with their teams and in their production environment today-they have all

highly skilled individuals, but how do they operate as a team, and how do they operate under pressure? CEO Ross Brewer discusses how businesses in the region can protect their strategic assets and key data in the context of accelerated digital transformation and the plans that SimSpace has for the region.

Our focus article on offensive security, by Satykam Acharya, Director Red Team, Infopercept Consulting Pvt Ltd examines how, just like in grammar, in order to avoid silly mistakes, organisations should have an offensive first and offensive daily approach to find their silly mistakes. Our interview of the month, with Harish Chib, Vice

President MEA at Sophos, discusses how Sophos Intercept X with XDR combines anti-ransomware technology, deep learning artificial intelligence, exploit prevention, and active adversary mitigations to stop attacks.

As you can see, this month's issue is power-packed. Aside from the special interviews, we also have the regular insight and opinion columns and news updates. So, make sure you don't miss out, Happy Reading!

GEARING UP TO FACE ATTACKERS

EVENTS



FOUNDER, CPI
Dominic De Sousa
(1959-2015)

Published by **CPI**

ADVERTISING
Group Publishing Director
Kausar Syed
kausar.syed@cpimediagroup.com

EDITORIAL
Editor
Anita Joseph
anita.joseph@cpimediagroup.com

PRODUCTION AND DESIGN
Designer
Prajith Payyapilly
prajith.payyapilly@cpimediagroup.com

DIGITAL SERVICES
Web Developer
Adarsh Snehan
webmaster@cpimediagroup.com

Publication licensed by
Dubai Production City, DCCA
PO Box 13700
Dubai, UAE

Tel: +971 4 5682993

Publishing Director
Natasha Pendleton
natasha.pendleton@cpimediagroup.com

Online Editor
Daniel Shepherd
daniel.shepherd@cpimediagroup.com

Sales Director
Sabita Miranda
sabita.miranda@cpimediagroup.com

© Copyright 2023 CPI
All rights reserved

While the publishers have made every effort to ensure the accuracy of all information in this magazine, they will not be held responsible for any errors therein.

SENTINELONE TO SPOTLIGHT INNOVATIVE XDR, IDENTITY AND EDR SOLUTIONS AT GISEC 2023

SentinelOne,

the global leader in autonomous cybersecurity, announce that it will be participating in the Gulf Information Security Expo & Conference (GISEC) 2023 being held from 14-16 March 2023 at Dubai World Trade Centre.

With a range of autonomous cybersecurity solutions, SentinelOne helps organizations stay ahead of emerging threats and protects their digital environments with confidence. The company will showcase its Extended Detection and Response (XDR) platform, Singularity XDR, as well as Singularity for Identity, an Identity Threat Detection and Response (ITDR) solution and Singularity for Endpoint, an endpoint detection and response (EDR) solution. As part of its plans for regional growth, SentinelOne has a number of objectives for the three-day event, including networking with potential clients and channel partners in the region.

"As a leader in next-generation endpoint protection, we look forward to showcasing our solutions and sharing our expertise with visitors and industry players alike at GISEC 2023," said Tamer Odeh, Regional Sales Director, SentinelOne. "It is one of the largest security exhibitions in the Middle East, and our team is keen to demonstrate how our autonomous cybersecurity platform can help organizations stay ahead of emerging threats and secure their digital environments with confidence."

At GISEC 2023, SentinelOne will highlight its flagship platform, Singularity XDR, a unified platform designed to provide comprehensive endpoint protection to users. The platform can autonomously supercharge, fortify, automate and extend protection from the endpoint to beyond, with unfettered visibility, proven protection, and industry-leading responsiveness.



SOPHOS NAMED A LEADER IN 2022 GARTNER MAGIC QUADRANT FOR ENDPOINT PROTECTION PLATFORMS

Sophos, a global leader in innovating

and delivering cybersecurity as a service, has announced that it has once again been named a Leader in the 2022 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP). This is the 13th consecutive time that Sophos is positioned as a Leader in the report.

Sophos' leading endpoint solution, Sophos Intercept X, protects more than 300,000 organizations against today's most advanced cyberthreats with deep learning malware detection, anti-ransomware, anti-exploit, and much more. The offering's new adaptive active adversary protection mode automatically disrupts attackers, providing security experts with time and insights needed to respond and remediate threats through Sophos XDR (extended detection and response). Health check capabilities further monitor and correct security configuration changes, enabling organizations to promptly re-establish security best practices.

"The threat landscape is too complex and changes too quickly for most organizations to defend against on their own, and they



need help from specialised security experts at scale to augment their frontline defenses," said Raja Patel, senior vice president of products at Sophos. "Endpoint security solutions are essential for attack prevention; however, the reality is that organizations often have environments with a mixture of security solutions, which could leave gaps in coverage. To correlate attacker behaviors across disparate technologies, Sophos delivers Sophos MDR with breakthrough vendor-agnostic capabilities, allowing us to detect and respond to active attacks across a customer's environment. We've removed the technological barriers that have historically limited what managed security services can handle, revolutionizing the way that MDR is delivered to produce superior security outcomes."

NOZOMI NETWORKS CONTINUES TO TRANSFORM OT AND IOT SECURITY SOLUTIONS AT GISEC 2023

Nozomi Networks, the leader in operational

technology (OT) and Internet of Things (IoT) security, will be participating at the upcoming Gulf Information Security Expo & Conference (GISEC) from 14-16 March 2023 at the Dubai World Trade Centre. At the exhibition, the company will highlight how its extensive suite of leading OT and IoT security solutions can be leveraged to protect critical infrastructure, industrial networks, and government organisations from cyber threats, all while maximizing operational resilience.

"We've observed an increase in demand for OT and IoT solutions in the Middle East, and both the public and private sectors are stepping up to strengthen defenses. Robust cybersecurity is of top

priority as OT and ICS systems embrace new technologies to stay ahead of the competition," said Bachir Moussa,

Regional Director – MEA, at Nozomi Networks. "Our solutions deliver exceptional network and asset visibility, threat detection, and insights for OT and IoT environments, allowing organisations to reduce risks and build cyber resilience. We are at GISEC 2023 to engage with companies facing similar challenges, existing and prospective customers, partners, and visitors from all around the world."



OPSWAT TO SHOW REGIONAL INDUSTRY PLAYERS THE ROUTE TO IT/OT SECURITY MATURITY AT GISEC 2023

OPSWAT, a global leader in critical infrastructure protection (CIP) cybersecurity solutions, has announced that it will be at GISEC 2023 to show the region's private and public sector enterprises how to develop their cybersecurity maturity through the company's end-to-end IT/OT security solutions.

"OPSWAT has been a GISEC attendee for many years, and this time around, we exhibit amid a threat landscape that is bubbling with risk for OT (Operational Technology) and ICS (Industrial Control System) environments," said Sertan Selcuk, Vice President of Sales, Middle East, Turkey, and Africa, OPSWAT. "Our mission to protect critical infrastructure through purpose-built CIP technologies has never been more urgent. Regional nations have

been hard at work diversifying their economies, and heavy industries such as utilities, energy, manufacturing and oil and gas can only innovate as long as they remain protected from cyber criminals."

"No single vendor provides anti-malware and sanitization solutions that cover file entry points across USB, Web traffic, storage, email and everything in between... except OPSWAT," Selcuk said. "We offer purpose-built CIP technologies rather than repurposed IT products — solutions that can be deployed in the cloud, on prem and in air-gapped networks, offering more flexibility than any other provider in the market."



CLOUDFLARE TO HIGHLIGHT ZERO TRUST ACCELERATION, DDOS MITIGATION AND PROTECTION OF CRITICAL INTERNET PROPERTIES AT GISEC GLOBAL 2023

Cloudflare, Inc, the security, performance, and reliability company helping to build a better Internet, has announced its participation at GISEC Global 2023.

The company will use the event as a platform to educate regional enterprises and organisations about protecting, consolidating and optimising their corporate networks, their IT and internet presence without the cost and complexity of managing legacy network hardware.

Bashar Bashairreh, Managing Director of Middle East & Turkey at Cloudflare said: "Over the past few years, ransomware, data breaches, and other cyberattacks have been hugely disruptive and cost businesses and public agencies huge amounts of money, in addition to loss of reputation and market trust. In response, as organisations embrace digital transformation and move their operations to the cloud, they should be looking to an integrated service

offering security, performance, reliability and privacy as the key pillars of a successful digital transformation strategy. "As a company that is leading innovation, we are excited to be present at GISEC, to partner with enterprises in the region on their network transformation journey. Corporate networking has become overly complicated. Network and IT teams that used to maintain "castle-and-moat" architectures are now responsible for much more: managing legacy WAN connectivity, establishing secure remote access, and stringing together disparate networking hardware on-premise to satisfy security, performance, and reliability needs. With Cloudflare, enterprises can have a single global platform that provides built-in, software-defined Zero Trust functionality, DDoS mitigation, firewall services, and traffic acceleration."



BEYONDTRUST INTELLIGENT IDENTITY & ACCESS SECURITY SOLUTIONS NOW AVAILABLE ON MICROSOFT AZURE MARKETPLACE

BeyondTrust, the worldwide leader in intelligent identity and access security, has announced the availability of BeyondTrust Password Safe and Privilege Management for Windows & Mac in the Microsoft Azure Marketplace, an online store providing applications and services for use on Azure. Customers can now take advantage of the productive and trusted Azure cloud platform, with streamlined deployment and management. This furthers BeyondTrust's commitment to giving customers choice and flexibility in purchasing its identity security solutions. Customers can expect a simplified procurement process through Azure Marketplace with flexible payment terms, consolidated billing, committed cloud spend burn-down, and enterprise discounts.

"BeyondTrust is committed to making it easy for customers to adopt and implement BeyondTrust solutions," said Brent Thurrell, Chief Revenue Officer at BeyondTrust. "As organizations increasingly pursue hybrid or multicloud strategies and expand cloud infrastructure, CISOs and IT decision-makers seek greater flexibility in purchasing and deploying chosen security solutions. By enabling them to quickly and easily leverage their existing Microsoft Azure commits, we can help customers accelerate their identity security journey and defend against cyberthreats."





ENTRUST IDENTIFIED AS AN OVERALL LEADER IN KUPPINGERCOLE COMPASS PASSWORDLESS AUTHENTICATION REPORT

LEADERSHIP STATUS IN PRODUCT, INNOVATION, AND MARKET CATEGORIES UNDERPIN ENTRUST'S
POSITION AS MARKET CHAMPIONS IN THIS GROWING SECTOR



THE ENTRUST IDENTITY AND ACCESS MANAGEMENT SOLUTION OFFERS MULTIPLE HIGH ASSURANCE PASSWORDLESS OPTIONS, ONE OF WHICH IS THE MOBILE SMART CREDENTIAL WHICH USES PKI BASED CRYPTOGRAPHIC KEYS COMBINED WITH BIOMETRIC AUTHENTICATION

the reliance on passwords and the inconvenience of legacy MFA.” The report also highlights the company’s global presence and partner ecosystem as an enabler for delivering its solutions.

“Passwordless authentication is finally gaining widespread adoption, removing the need for passwords completely,” said Alejandro Leal, Research Analyst at KuppingerCole. “Although we’re seeing them implemented by more and more enterprises and even consumer-facing businesses, for many organizations this technology can be confusing and obscure. Our report is designed to help organizations find the technology providers with the best overall product, functionality, innovation and market vision for this category. As an overall leader, Entrust Identity credentials can be tailored to meet the needs and preferences of users.”

“For years, IT professionals have discussed the idea of passwords becoming obsolete. The issue with passwords is that they can easily be stolen and compromised. By replacing passwords with a high assurance passwordless solutions with proximity-based factors, organizations can effectively protect users against remote based account take over (ATO) attacks,” said James Lapalme, Vice President of Identity at Entrust. “By placing Entrust as a leader in passwordless authentication, KuppingerCole is validating our commitment to building best-in-class high assurance passwordless authentication solutions that can provide secure access with strong authentication for workforce, consumer and citizen use cases. Furthermore, high assurance passwordless can form a central part of a Zero Trust framework establishing an identity centric

approach to security. Having a mature zero trust framework with trusted identities not only produces considerable advancements in security, but also lowers costs and complexity while offering more peace of mind for cybersecurity teams, business and IT leaders, and end-users.”

The Entrust Identity and Access Management solution offers multiple high assurance passwordless options, one of which is the mobile smart credential which uses PKI based cryptographic keys combined with biometric authentication, such as fingerprint or facial recognition over Bluetooth to ensure strong proximity-based authentication that is resistant to remote based ATO attacks. This ensures that the credential holder is, in fact, the credential owner, protecting workers’ digital identities and corporate assets. Capabilities highlighted in the report include issuing credentials that utilize their mobile device, including mobile push authentications, one-time passwords (OTPs), FIDO keys or smart credentials secured by PKI. The platform also includes an innovative proximity-based authentication capability that allows for email signing and encryption. In addition, Entrust Identity adaptive risk engine evaluates device type, IP address, geo-location and velocity, and user attributes to assess whether risk level during an authentication request from a user is below a defined threshold and take corresponding actions to issue a new authentication challenge requiring a new MFA authenticator or denying the request.”

In addition, Entrust IAM also supports the latest FIDO Passkeys capability that aim to accelerate the journey to passwordless especially for customer IAM use cases. 🔑

Entrust, a global leader in trusted payments, identities, and digital infrastructure, has been cited as an Overall Leader in analyst firm KuppingerCole’s global 2022 Leadership Compass for Passwordless Authentication. The report provides an overview of the market for Passwordless Authentication products and services and contributing to the overall leader standing, Entrust appears as a leader across all three product, market, and innovation categories.

According to the report, “Entrust Identity and Access Management has an innovative set of capabilities for customers who need high security assurance authentication. For organizations that broadly utilize Entrust solutions, the Entrust Identity as a Service is a compelling option for organizations wishing to eliminate



ALL SOPHOS OFFERINGS ARE POWERED BY THREAT INTELLIGENCE FROM SOPHOS X-OPS, A CROSS-OPERATIONAL TASK FORCE LINKING SOPHOSLABS, SOPHOS SECOPS AND SOPHOSAI.

SECURITY FIRST

HARISH CHIB, VICE PRESIDENT MEA, SOPHOS TELLS ANITA JOSEPH ON THE THREAT LANDSCAPE, RANSOMWARE, CRYPTOROM SCAMS AND XDR.

Managed Detection and Response (MDR) is now more relevant than ever. What is the USP of Sophos' Managed Detection portfolio as compared to other MDR providers, in a market that is crowded and competitive?

Superior adversary insights, attack visibility, and response expertise deliver unparalleled threat detection, neutralisation, and response for our customers.

- o Supporting over 15,000 organisations means we see and stop a plethora of attacks, in both volume and variety, on a weekly basis.
- o We secure hundreds, sometimes thousands, of similar organisations, our customers directly benefit from ever enhancing and unparalleled community immunity.
- o Sophos MDR is backed by the world-leading Sophos X-Ops team, a group of over 500 highly skilled threat intelligence, data, and SOC operations experts' organisations in each industry sector. By constantly sharing attack learnings across
- o , acting as the ultimate SOC extension and multiplier for our customers and partners.

- o Our patented protection technology, combined with our unique 3rd party data processing pipeline, SOAR playbooks and incident response expertise, means we excel across the full "protect, detect, respond, recover and learn" lifecycle.
- o Our full environment detection and response means we get visibility of attacks, enabling us to see and then stop them, quickly and effectively. Sophos MDR ingests, normalises, and correlates telemetry from endpoint, firewall, network, email, cloud and identity security solutions, enabling us to detect and respond to adversaries as early as possible within the kill chain.

Flexible, customer-focused solutions designed for today's complex operating environments complement and enable our customers' businesses.

- o Sophos MDR can work with our own security solutions, third-party solutions, or any combination of the two. This unique flexibility maximises existing security investment ROI, facilitating and enabling long-term security strategies.
- o As each customer requires different levels of support, Sophos MDR allows organisations to choose the most appropriate and relevant engagement model for their needs. From notifying a customer about incidents so they

can fully manage the response in-house, through to responding together, or having the Sophos team fully take care of it with minimal customer involvement, Sophos MDR offers unparalleled flexibility to customers.

- o Unlimited incident response at no additional cost ensures that when an incident occurs, customers have the reassurance that the situation will be fully taken care of, without losing sleep over hours and subsequent charges piling up.
- o Our skin-in-the-game \$1 million breach protection warranty provides peace of mind to business leaders and IT teams alike. We underwrite the warranty ourselves, as opposed to the market norm of outsourcing to a 3rd party insurance provider, further demonstrating the utmost levels of confidence we have in our service delivery.

XDR is now in the limelight. Tell us about the Sophos XDR platform.

Sophos Intercept X with XDR combines anti-ransomware technology, deep learning artificial intelligence, exploit prevention, and active adversary mitigations to stop attacks. All Sophos offerings are powered by threat intelligence from Sophos X-Ops, a cross-operational task force linking SophosLabs, Sophos SecOps and

SophosAI, and are easily managed in the cloud-native Sophos Central platform or by Sophos Managed Detection and Response, a 24/7 managed detection and response (MDR) service used by more than 15,000 organisations.

Sophos recently added the ability to integrate vendor agnostic telemetry from third-party security technologies into its MDR service, providing unprecedented visibility and detection across diverse operating environments. The same vendor agnostic telemetry integrations will be available in the Sophos Intercept X Advanced with XDR in 2023.

How is EDR different from XDR? What exactly must businesses look for while choosing an XDR platform?

With Endpoint Detection and Response (EDR), the focus is primarily on Endpoints and should start with the best real-time protection. While an Endpoint can provide Security Analysts with vast details about an attack, it only provides visibility on devices where Endpoint Protection is installed. Additionally, a modern organisation has more than endpoints. There will be multiple security controls, including some identity components, network infrastructure, email and messaging products, some elements of operations already in the cloud, and potentially more.

Extended Detection and Response (XDR) expands the EDR concept to provide a holistic view across an organisation by including detections and telemetry from the other security controls in an organisation. When choosing an XDR solution, there are five key areas to consider. Integrations, detections, investigations, automation, and response capabilities.

Ensure the XDR solution integrates detections and telemetry from your existing security controls to give you the visibility required. To stop your team from drowning in alerts, it must analyse, group, and grade the detections across all security controls to help identify where your team should spend their valuable time. Look for strong

investigation capabilities that allow you to group related detections and cross-reference indicators of compromise from multiple sources. Automating protection and other repetitive tasks will help your team scale to complete investigations and remediation tasks faster. Once the investigation phase is complete and the threat is understood, the XDR solution must have extensive response capabilities. Attackers are creative in their approach; you don't need limitations in your ability to respond.

Ransomware as a threat is taking on deeper, more complicated dimensions as time goes by. How has it evolved in the last one year or so?

The Sophos Whitepaper, "The State of Ransomware 2022" has many great statistics and insights. The Ransomware challenge facing organisations continues to grow. It is important to remember that Ransomware is one part of a complex attack chain, positioned as one of the final steps, and is remembered due to its highly visible and disruptive nature. The steps before the delivery of ransomware (use of legitimate identities, use of exploits, living off-the-land techniques to avoid detection, etc.) revolve around remaining invisible and have also evolved over the last year. Stopping an attacker early in the attack chain reduces the costs and impact on an organisation. Many organisations have realised that cybersecurity is so complex, difficult, and moves so fast that they can't manage it effectively on their own. Managed Detection and Response services have evolved in size and popularity as they provide the detection and response capabilities to ransomware and the various TTPs used to distribute it to organisations.

Please elaborate on the latest findings by Sophos on CryptoRom scams

We've had multiple findings. First, we found that two fake apps supporting these scams had gotten into the Apple App Store and Google Play app store (we recently found a third using the same

technique). Second, we engaged two separate Sha Zhu Pan ("Pig butchering") scams that approached me through lures on social media and text messages, and uncovered their operating tactics and tools. One was using a legitimate trading app that had been modified to connect to a fake gold trading market; the second was using fake crypto trading apps to defraud victims and had collected over \$3 million US in cryptocurrency over a three-month period. We found multiple additional scams using the same tools as these two scams.

Sophos has been tracking and reporting CryptoRom scams for two years now, how has the tactics of scammers changed over time?

They are diversifying. We still see romance-based approaches being used to lure victims, but they are also using other avenues—including AirBnB, where one victim was approached initially under the guise of renting his property. They are shifting in some cases away from crypto-based scams toward fake commodity, foreign exchange and stock trading. And some of the apps are becoming more sophisticated and more closely mirroring real world brands. Also, this is the first time we've seen CryptoRom apps make it into the Apple App Store.

Please tell us more about the first fake CryptoRom apps- Ace Pro and MBM_BitScan which Sophos reported.

Ace Pro was advertised as a QR code scanning application, and MBM_BitScan claimed to be a cryptocurrency tracker. Both applications retrieved some of their content from a remote website. After they had been approved and posted to the App Store, the website they connected to was changed to deliver content from another location, turning them into fake crypto trading apps. We found a third app called BerryX in the App Store that used the same bypass technique; it claims in the App Store listing to be a reading app.

We have alerted Apple and Google to these apps, and they have been removed. 🙋



presents

INFOSEC & CYBERSECURITY

CONGRESS 2023

HABTOOR GRAND RESORT,
AUTOGRAPH COLLECTION, JBR DUBAI

2ND MARCH 2023

CPI Media Group and **tahawultech.com** in conjunction with **ISACA UAE** would like to place on record our sincere thanks to ALL our sponsors for making the **Infosec & Cybersecurity Congress Dubai** an incredible success.

Your support allowed us to bring together the key security stakeholders from across the UAE, in a bid to tackle the current issues at hand

A big congratulations to ALL our award winners who were recognised for their outstanding contributions to tackling the biggest issues in the cybersecurity space.

Thank You Sponsors

PLATINUM SPONSOR



THREAT DETECTION TECHNOLOGY PARTNER



GOLD SPONSORS



OFFICIAL PUBLICATIONS



HOSTED BY



ORGANISED BY



#infosec&cybersecuritycongress2023

#tahawultech #isacauaechapter

BATTLE READY

ROSS BREWER, CHIEF REVENUE OFFICER AT SIMSPACE, TELLS ANITA JOSEPH HOW THE COMPANY HELPS BUSINESSES WITH CONTINUOUS SECURITY IMPROVEMENTS AND DELIVERS QUANTITATIVE AND ACTIONABLE INSIGHTS INTO HOW ORGANISATIONS CAN PROTECT CRITICAL ASSETS AGAINST CYBER THREATS.

Tell us about SimSpace and your business and offerings.

SimSpace comes from our founder, Hutch, who was an F-15 fighter pilot. He then went into the Pentagon and later to one of the three-letter agencies and was asked by General Alexander, who was the 4-star general that set up Cyber Command to build out a training capability for the US Military. He was joined by Lee Rossey, who is our co-founder. Lee was with Lincoln Laboratory as part of MIT. He specialised in building simulation environments. So, they created SimSpace, the platform, which is our Cyber Force Platform, and it is broken down into three offerings. We provide military-grade cyber rangers, elite force training, and live fire

exercises. And this is what we built for the US Cyber Command that we are now making available to allied organisations and countries, and critical national infrastructure throughout the region.

Tell us how you help organisations develop their cybersecurity teams to protect strategic assets and manage risk overall.

We help organisations move from several maturity aspects. If you take financial services as an example, they are looking to move beyond the classic Capture-the-Flag table topics or size to where

they want to do live team sort of mission rehearsal, just like the military does.

So, we provide cyber ranges that help organisations, institutions, and critical national infrastructure, do exactly that. Last week, we were in the Gulf region, at a country level working with one of the big four auditors. We were supporting an event they held, which was a national war game exercise for you know for country-level Financial Services Group of the top bank. They were run through a two-day technical exercise and immersive technical exercise using SimSpace and then a business exercise for the executives for the following day. We are looking to sort of repeat this with leading financial services organisations throughout the Gulf now.

So, what we do is help organisations answer several sophisticated complex questions they can answer with

HUMAN IS OUR BEST LINE OF DEFENCE, BUT IT'S ALSO OUR BIGGEST WEAKNESS.



their teams and in their production environment today; they have all these highly skilled individuals, but how do they operate as a team? And how they operate under pressure.

For instance, in one of the biggest banks in the world, last October, we did a 24-hour event where we collapsed three years of attacks into a 24-hour window, and their organisation wanted to see how the shift pattern handover would work. There were three, eight-hour shift patterns within that 24-hour window. And we put the team through its paces. It helps organisations understand the communications, the delegation, the collaboration, that sort of human skills, if you will, on whether they are going to be up to the required sort of strength in time of need, i.e., when there's a serious attack.

Tell us about cyber ranges. How critical is it to an organisation's comprehensive security readiness program? And what are the different cyber ranges delivery models? And how does the simulation work for customers?

Cyber Ranges help organisations answer several questions about the people, processes, and technology that they are struggling to answer in their production environments today. There is testing that goes on to test controls. And I come from a background in that industry segment myself. However, with a range, it creates a sort of a consequence-free, safe environment that organisations can work in, and turn up the heat if you will.

So, in production, if you want to do some red teaming, or some penetration testing, or some activity in production, you might be able to turn the volume up too; but you don't want to break anything,



you don't want to break the people and you don't want to create too much noise, that it blinds the security operations center to their normal activities.

So, by using a range, which is separate from production, you can turn the temperature up and test technologies and people and processes to that sort of much higher impact level. The range also has the additional benefit of being able

to do all sorts of things within that range and answer all kinds of sophisticated questions for instance, they might be looking to rationalise the number of security controls they have. So how might they overlap? And obviously, a lot of security controls mean complexity. So how can they reduce that complexity, and know that they can swap some of the tools out to reduce the cost of them without losing protection, and without losing the overall effectiveness of their capability? So, there are many use cases for the range and the delivery models can be provided as software – as a hosted solution or can be provided with the hardware.

Now, a lot of the critical national infrastructure work, Ministry of Defence

CYBER RANGES HELP ORGANISATIONS ANSWER SEVERAL QUESTIONS ABOUT THE PEOPLE, PROCESSES, AND TECHNOLOGY THAT THEY ARE STRUGGLING TO ANSWER IN THEIR PRODUCTION ENVIRONMENTS TODAY.



work, and intelligence community work that we do, these organisations want to be in control of the data. And they want to be in control of the assets. So, these are typically close. They're not connected

THE GREAT THING ABOUT THE REGION IS THAT MOST OF THE ORGANISATIONS WANT THE BEST AND THEY WANT TO MOVE TO THE HIGHEST LEVEL OF CAPABILITY THAT THEY CAN.

to their production network. They're not connected to the internet. And they're often you know, the old traditional on-prem-approach if you will.

SimSpace recently announced its expansion in the MEA APJ markets. What opportunity do you see in the Middle East market and in which segments specifically?

Well, as I said, in February, I was in the region in Saudi, UAE, and other countries, and we were looking to appoint our distributor in the region. The announcement will come from that in the coming period here. And there's a huge opportunity because if you look at the LEAP conference, as an example, I managed to attend that on the first day.

By four o'clock, there was a notification, and as I was leaving to go from the conference to the airport, I saw hundreds of people milling around the doorways and I thought, this is interesting; there must be some dignitaries here and the crowd is here to see the dignitaries. But it turned out that there was a notification to say that they closed the doors because they had too many people at the event at four o'clock on the first day! So, if you look at the amount of activity and volume of cybersecurity work that's going on in the region, especially in the Kingdom of Saudi Arabia, we have a huge opportunity.

The great thing about the region is that most of the organisations want the best and they want to move to the highest level of capability that they can. And that

fits nicely with what we're doing around helping organisations sort of move to this sort of continuous security improvement model that we can do by not only providing training for the individuals but training for their teams. These exercises measure and show progression and maturity over time as we continue to do this.

The Middle East cybersecurity market size is projected to grow from USD 20.3 billion in 2022 & to USD 44.7 billion by 2027. So how do you see SimSpace planning to utilise this huge opportunity? And what are your plans for the region, anything that we should look forward to?

Well, we've got a huge history in the region. We've been very successful there with previous organisations and previous teams. And then with that growth, I've always made it very clear to my colleagues around the world that in terms of the Gulf region, it's a little

WHAT WE DO IS HELP ORGANISATIONS ANSWER SEVERAL SOPHISTICATED COMPLEX QUESTIONS THEY CAN ANSWER WITH THEIR TEAMS AND IN THEIR PRODUCTION ENVIRONMENT TODAY.

unique, and as much that it's still in sort of infrastructure, sort of creation and infrastructure-build mode; where I would see some of the other countries, maybe in Europe, maybe even in the US, to a certain extent, where it's more in maintenance mode, you know. All the highways were built in the US in the 50s. And they're all there. So, if you're driving a concrete truck, and in the 50s, you were a very wealthy person, and you had a lot of work to do well, whereas you look at cybersecurity in the Gulf, it's at that stage of, it's a huge market already. And it's going to double in size. And it's the sort of a hidden gem, if you will, for cybersecurity companies that understand

that and know how to operate through partners and know how to support the market culturally and locally in a way that you need to be successful.

If you can, sort of unlock that lock with the right key, it can be a phenomenally successful market. And so, you know, hiring local teams, knowing the local culture, local talent, is critical. And watch the space as we develop and expand and do all the things that we've done in the past to make the region so successful. And in my previous roles, we've even got to the point where the Gulf region produced as much as 50% of the global revenues for a company, which given the size of the market, that's a huge outcome.



Cyber threats are a constant concern, so how do you prepare for the future? As far as threats, which may not be existent now, what are the unique threat trends or trends specific to this region that you intend to focus on? And how do you ensure that the talent acquired for the same remains versatile and equipped to face new challenges?

I think that's an important question and AI is going to be a huge factor in what's going on. And we've heard a lot about chatGPT, or whatever AI technology you want to talk about. I think there are some risks around that, that people may be getting a little bit lazy and programming and using these kinds of tools to provide code for them.

Potentially, there's a MEL training aspect to those technologies where you could create a world where you sort of MEL-train the AI so that it's producing code that's got embedded vulnerabilities in it. There's a risk there



these technologies are not designed to check the code. They're just designed to produce what they've heard about and what they think they've been told is good, right?

So, I think AI quantum computing is going to make a big difference, but that's not going to be in the short term that's going to be in the medium term, but people need to think about that because that's going to have a big impact on the algorithms. And that's going to fundamentally change all the security. I'm not sure that's in the next one to three years, it's probably more than the three-to-five-year range.

But I think AI in the next one to three years, can bring in what I call the Wuhan of cybersecurity. Before you know it, you've got the snowball effect of slowing down the internet and chewing up a whole lot of resources, because this thing gets out of control. And, as you know, is propagating around the internet. But I think we need to come back to just the reality here, of the big digital hygiene

AI QUANTUM COMPUTING WILL MAKE A BIG DIFFERENCE.

problem in the industry. And people need to focus on the basics.

This is making sure that the teams are trained on the technologies that they have. If you look at the data breach investigation report of Verizon, two years ago, they said that 85% of breaches stemmed from a human failure. So, human is our best line of defence, but it's also our biggest weakness. So, I think the shift must happen, where we put increasingly more effort into our resources, training them as individuals, training them as teams, testing them under pressure, identifying their weaknesses, and then filling those weaknesses with people processes or additional training. 🧑

SECURING BUSINESS EMAILS

WERNO GEVERS, REGIONAL MANAGER, MIMECAST MIDDLE EAST, TELLS ANITA JOSEPH HOW THE COMPANY HELPS ORGANISATIONS IMPLEMENT A COMPLETE, HOLISTIC STRATEGY TO REDUCE BUSINESS EMAIL COMPROMISE RISK.

ORGANISATIONS NEED A COMPREHENSIVE, LAYERED STRATEGY FOR RESISTING BEC ATTACKS.

How does Mimecast's advanced email and collaboration security optimise efficacy and help make smarter decisions

about communications that fall into the gray area between safe and malicious?

Mimecast uses AI and Machine Learning models based on our analysis of more than 1.3B emails daily. By filtering out malicious emails at scale and driving intelligent analysis of the "unknown", Mimecast's advanced email and collaboration security makes information actionable and provides the reliability, resilience, and scale that the modern threat landscape demands. Our solutions take the guesswork out of threat detection and by applying the right detection capabilities at the right time, we are able to offer continuous protection, letting end users work protected, without interrupting their jobs.

Tell us more about the Mimecast X1 platform and how it's providing the resilience, reliability and scale that the modern threat landscape demands?

The widespread adoption of hybrid work environments coupled with the increased use of digital-centric communication channels has expanded the attack surface – creating new organisational security risks for both people and data. The Mimecast X1 Platform is designed to mitigate risk across email communications and help empower organisations to secure their workplace environment wherever work happens. It does this through various key methods, such as using AI and machine learning to detect emerging and unknown threat types, as well as offering a vast API ecosystem that supports fast, simplified integration of Mimecast with existing security investments.

Business Email Compromise (BEC) is said to be the costliest of Internet crimes, accounting for 44% of the \$4.1 billion in US losses reported in 2020. How does Mimecast help organisations

implement a complete, holistic strategy to reduce BEC risk?

There are several ways that organisations can prevent BEC attacks from reaching both their own employees and their customers and partners:

1. Organisations can leverage Mimecast's AI-based Brand Exploit Protect and DMARC Analyzer tools to monitor and respond to malicious brand impersonation attacks out in the web and through email. The DMARC protocol gives an organisation full visibility and control of who sends emails on their behalf and protects against BEC phishing attacks that seem to originate within your organisation but were actually crafted by criminals.
2. Invest in regular and impactful cyber awareness training for staff, as it is one of the most effective ways of strengthening an organisation's overall cyber resilience. Empowering employees to understand email threats and be more vigilant will help them resist advanced and targeted threats like BEC.
3. Mimecast's Secure Email Gateway with targeted threat protection is an essential tool in helping to protect employees from these impersonation attacks. Every inbound message is analysed in real time for signs of risk, from sender spoofing to suspicious international characters or body content. Threat intelligence can then be shared instantly across the security stack, empowering all security systems to respond more quickly and effectively.

How can and should, organisations respond to Business Email Compromise, should it happen?

Organisations need a comprehensive, layered strategy for resisting BEC attacks. Central to deterrence, is effective, continuous security awareness training to compel attention, engage employees, and clarify the right actions to take when confronted with a possible attack. Training should be linked to strong policies – for example, independently verifying every request to change a payment account.

Should a BEC attack occur, an organisation should immediately trace

and quarantine the affected user's email and associated credentials, and perform a full audit of all internal and external messaging to curb the spread of any further malicious emails. From there, security teams can trace if any internal systems have been compromised and take steps to further stop remote attackers from gaining access to other connected systems. Once all traces of the BEC attack have been dealt with, the user's access can be restored after following relevant security protocols.

What are some of the threat-security patterns/trends businesses in the Middle East must watch out for in 2023?

This year is likely to be another busy year in the cybersecurity space and cyberthreats will continue to evolve and become more dangerous. But here is a snapshot of some of the key trends Mimecast's security experts predict we will see:

- With new employees joining companies at the beginning of the year, there will be an increase in phishing attacks that are engineered to look like congratulatory emails from senior executives. New hires may receive an influx in emails that masquerade as LinkedIn connection requests or onboarding information, but are in fact fake landing pages to harvest credentials for account takeover fraud.
- As a significant portion of the workforce continues to work from home, companies may roll out tighter BYOD policies, or offer separate home networking equipment.
- Combating ransomware will continue to be a top priority for organisations, and it is important that businesses' ransomware defences are kept up to date as well.
- In 2023, threat actors are likely to take social engineering to the next level. As AI voice cloning technology becomes more powerful and readily available, we will see an increase in impersonation attacks that utilise audio deepfakes. These will be used in combination with compromised email and collaboration accounts. 🗡️

Secure Your **Digital Future**

Simple. Secure. Resilient.



**Secure Your Enterprise IT Footprint
For A Safer Digital Journey**

www.raqmiyat.com

UAE | KSA | INDIA

Security

ADVISOR

MIDDLE EAST

protiviti



SPECIAL REPORT

UNDERSTANDING DATA PRIVACY

UNDERSTANDING DATA PRIVACY

I SENIOR LEADERS AT PROTIVITI MEMBER FIRM FOR THE MIDDLE EAST REGION DISCUSS WHAT DATA PRIVACY MEANS IN THE CONTEXT OF TODAY'S COMPLEX DIGITAL TRANSFORMATION LANDSCAPE AND HOW THE FIRM IS PROACTIVELY HELPING ORGANISATIONS SECURE THEIR CRITICAL DATA AND ASSETS.

How has the concept of data privacy evolved and what are some of the trends today?

Arindam De, Deputy CEO and Managing Director

Our regional as well as global clients are experiencing unprecedented shifts in their data privacy landscapes. Recently enacted state regulations and the increasing prospect of additional state and federal privacy laws – not to mention the kaleidoscope of rapidly expanding privacy regulations globally – are forcing business to implement technical, legal and operational changes on a continuous basis. These changes are not necessarily exclusive of one another and often overlap, resulting in highly complex legal and regulatory scenarios. Additionally, consumers globally and especially in the Middle East, are becoming increasingly conscious of their privacy rights and expect enhanced transparency into how organisations process and store their personal data. Furthermore, data breach risks are also tracked as part of enterprise risk management programs and these concerns are often discussed in audit committees/ board meetings.

Organisations today recognise the need to establish a focused program to address

privacy requirements by establishing robust governance framework, strengthening data protection controls, embedding privacy requirements in their Mergers & Acquisition and third-party contracts. Key trends for data privacy -

1. Increased Consumer Awareness – Consumers are now minimally sharing their sensitive data, as they are becoming aware of the risks of leaked personal sensitive data being used for malicious purposes.
2. Data Privacy Program Compliance is time consuming – Data Privacy laws have already been published in Bahrain, Qatar, KSA and UAE, however, enforcement of these laws in some countries is work in progress. Clarity on Enforcement – All data privacy laws have defined hefty fines and even imprisonment. The key concern of the organisations is exposure to media in case of a breach and legal consequences such as imprisonment.
3. No longer a value add – Many

organisations, particularly those in the financial and healthcare sectors, have developed their privacy programs to gain consumer trust, whereas many organisations prefer to wait for the enforcement before investing in data privacy program implementations.

The frequency and magnitude of data breaches are increasing. So how important is data privacy today?

Niraj Mathur, Managing Director – Security & Privacy Solutions

Various reports have highlighted that over the last few years, the Middle East Region has been among the top 3 regions facing the highest cost of data breaches. Each year, these costs have been rising at an average rate of 12 – 15%.

These data breaches have not only resulted in organisations adopting data security best practices and strengthening their privacy controls. They have also increased awareness amongst consumers.

ORGANISATIONS THESE DAYS ARE RECOGNISING THE NEED TO ESTABLISH A FOCUSED PROGRAM TO ADDRESS PRIVACY REQUIREMENTS BY CREATING A ROBUST GOVERNANCE FRAMEWORK.

Going forward, this increased alertness will be one of the key factors for organisations to meet data privacy challenges more proactively, primarily because of the consequences that information leakage could have on their businesses.

Moreover, as organisations face increasing pressure to embrace digital technologies for meeting evolving consumer expectations, the importance of data privacy will keep rising in the coming years. As data becomes embedded in every decision, interaction, and process, managing data effectively and ensuring data privacy will prove crucial.

Many countries in the Middle East have introduced privacy laws, because of which the data privacy programs in organisations have increased in maturity. Organisations have also begun to realise that the lack of data privacy controls can have a negative

impact on their consumers' trust level and reputation. Consequently, we expect data privacy to be on the agenda of most organisations in 2023.

While cybersecurity is indeed a top priority in boardroom discussions, do you think a more targeted focus on data privacy is needed among security decision makers?

Harish V, Country Managing Director - UAE

While cybersecurity continues to be a matter of concern in boardrooms, a more targeted focus on data privacy is becoming necessary to ensure compliance across a rapidly expanding number of regulations. While cybersecurity will continue to be a core component for any data privacy program there are multiple facets including business processes, data governance, legal issues and regulatory compliance that require effective

collaboration to holistically address the privacy program's needs, e.g., re-engineering business process to collect consumer sensitive information, or marketing campaigns to address data privacy controls.

Additionally, for privacy stakeholders, upholding the rights of data subjects is a primary objective, while cybersecurity is focused on protecting the organisation's data. Therefore, striking the right balance becomes of the utmost importance. This requires focused and collaborative discussions between executive teams and the company's cyber and data privacy professionals, as regulatory scrutiny, the risk of cyberattacks and consumer demands for privacy protections continue to escalate. Data privacy will gain the attention of board members when the laws in respective countries are effectively implemented by the regulators.



Arindam De
Deputy CEO and Managing Director



Harish Visweswaraiah
Country Managing Director - UAE



Ranjan Sinha
Managing Director - Technology Consulting Solutions



Niraj Mathur
Managing Director - Security & Privacy Solutions



Siva S
Managing Director - Security & Privacy Solutions



Mohammed Arshad
Managing Director - Cloud Solutions

How about data visibility? Do businesses actually know what data they have and where exactly it resides?

Ranjan Sinha, Managing Director – Technology Consulting Solutions

Over the last few decades, technological advancements and business transformations have resulted in the collection and processing large volumes of data, including personal data. However, this underscores the need for greater visibility and control, specifically for personal sensitive data. For instance, in the BFSI sector, traditional paper-based transactions, continued use of legacy systems and the current transition to emerging technologies have resulted in a varied range of structured and unstructured data sets. This, coupled with the lack of formalised data governance and records management program, has made it difficult for many such entities to discover, control, and manage their data footprint.

In addition to knowing what their “crown jewels” are, organisations must understand what personal data they possess, whether appropriate privacy controls are in place, whether the data qualifies for data subject access or deletion requests, or have disclosure obligations associated with them. However, most organisations fail to have visibility over their data, including where the data resides. Conversations often lead to a realisation that data should be inventoried, cataloged and stored in a manner — structured or unstructured — that allows the organisation to determine whether the data is subject to privacy requirements in the jurisdictions within which it operates.

PROTIVITI HELPS BUILD THE FOUNDATIONS OF A STRONG BUT FLEXIBLE PRIVACY PROGRAM IN COMPLIANCE WITH REGIONAL DATA PROTECTION LAWS.



There similarly needs to be clear documentation and understanding of how personal data is collected and used in accordance with the organisations disclosures in its privacy notices and applicable regulatory obligations. Further, appropriate risk-based security controls should be implemented, such as access controls and encryption techniques.

Recurring data inventory and classification assessments are standard best practice

for all organisations that store personally identifiable information. Decision-makers should make it a point to find out from the management how the organisation leverages external parties to validate the appropriateness of privacy-related controls. As external auditors may force this conversation, the management should be prepared for this by inventorying high-risk data inside the organisation and determining that protected data is properly inventoried,



IDENTIFYING OWNERS FOR AN ORGANISATION'S CRITICAL DATA ELEMENTS AND KEY DATA ASSETS REMAINS THE TOP CHALLENGE IN MOST, IF NOT ALL, ORGANISATIONS.

Protiviti helps build the foundations of a strong but flexible privacy program that includes understanding principles, educating stakeholders and developing an applicable governance structure for managing changes. This base enables companies and their stakeholders to address the uncertain future of privacy regulations with greater confidence.

The Protiviti Advantage:

We start with the business problem – and apply the right solutions and technology to help achieve business value.

We support our clients through entire initiatives – from understanding business issues, to developing a strategy, to delivering the implementation and providing ongoing support.

Our methodologies are focused on holistically understanding risk – our approach goes beyond identifying gaps, issues or vulnerabilities. We determine root causes, validate issues and develop short-term and/or long-term recommendations.

Integrated approach – We integrate our technical and legal expertise with emerging technologies.

Technology accelerators – We leverage the intellectual property within our partner ecosystem to help fast track technology deployments.

Flexible delivery models – to address short term skill gaps, deliver projects or transform your organisation quickly and cost efficiently.

secured, shared and disposed of, as required by regulations or determined risk.

Protiviti provides expert-level data security and privacy management to companies in more than 27 countries. What's your approach?

Siva S, Managing Director – Security & Privacy Solutions

Protiviti applies a holistic framework that addresses the fundamental aspects of

data privacy, without being locked into any one specific compliance format. We focus on the most pressing data privacy issues companies face, including:

1. Developing strategies to address global data privacy regulations
2. Compliance with regulatory obligations
3. Addressing resource and skill shortages
4. Operationalizing privacy needs, and
5. Implementing privacy tools and remediation support

Privacy As A Service (Protiviti PRAAS™) - Overview



As part of the implementation support to support client in establishing their privacy program, Protiviti would carry out the following activities:

5 - Monitoring Privacy Legislation and Program Management

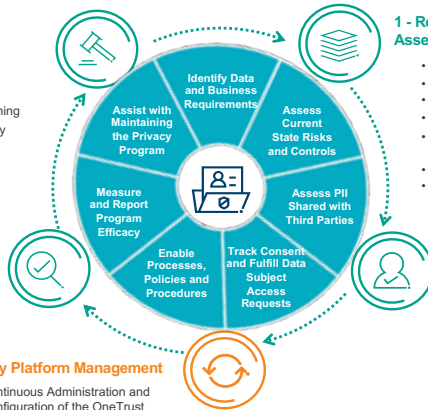
- Update Privacy Policies
- Update Privacy Controls Baseline
- Conduct Annual Awareness and Training
- Measure and Report Program Efficacy
- Maintain Privacy Notifications

4 - Privacy By Design Assessment & Engineering

- Perform Privacy Impact Assessments (PIAs)
- Perform Data Protection Impact Assessments (DPIAs)
- Support Privacy by Default & Design Engineering

3 - Privacy Platform Management

- Continuous Administration and Configuration of the OneTrust Environment



1 - Recurring Data Inventory, Classification and Assessments

- Maintain Inventory of Processing Activities
- Maintain Inventory of IT Systems and Data Classifications
- Maintain Data Maps
- Maintain Inventory of Privacy Obligations
- Conduct Compliance Assessments (GDPR, NIST DPF etc.)
- Conduct Data Protection Assessments
- Conduct Third-Party Assessments

2 - Data Subject Rights (DSR) Request Management

- Manage Request Intake and Workflow Process
- Manage Access Request Fulfillment Process
- Manage Third-Party Request Fulfillment Process
- Monitor Consent Management Practices

What is the importance of data quality and data governance in the context of data privacy?

Praveen Kokku, Managing Director – Data & Digital Solutions

By definition, data governance ensures that data is secure, private, accurate, available and usable. Without these as the guiding definition, every program will have blind spots, resulting in limited resonance value for business constituents. However, most data governance programs would be deemed successful if they address:

- Setting policies and procedures
- Data Quality (identification/ remediation)
- Technical Metadata and Business Glossary
- Data Lineage, and
- Operating models

The post-digital era has been driving data proliferation, and one would expect business decision-makers to leverage their data for insights. However, organisations are slipping into data chaos and business users are increasingly making decisions based on gut instincts, moving away from being analytics driven. Data Governance and Quality, therefore, have become boardroom priorities for most organisations, as they

continue to battle with the challenge of instilling confidence in data among business users and their ability to access and sustain effective and comprehensive data assets. Good data governance will allow organisations to transform into an Insight Driven Organisation (IDO).

While complete transformation into an IDO can be an aspiration, security and privacy by design are key, not just to avoid regulatory fines but to win the confidence of stakeholders (consumers, citizens, employees, shareholders and the board). The objective of an IDO is to democratise data and make it available as an office supply. It is therefore, mandatory to ensure that the right data ends up with the right owner. Miscreants (outside an organisation)

are constantly in attack mode. Therefore, an organisation's Chief Data Officer and Chief Security Officer must work hand-in-glove to secure and protect their organisation's data resources.

What are the 3 biggest challenges organisations face related to data quality, and what is Protiviti's approach to solving this problem?

Identifying the owners of an organisation's critical data elements and key data assets remains the top challenge for most, if not all, organisations. Businesses assume it is the responsibility of the Information Technology department (IT) to ensure authenticity of data, while the fact remains that data is 'of the business, generated by the business,' while conducting the business. The IT department is only the custodian of this data, and they manage the application storing the data. Then again, even when an organisation is successful in identifying data ownership, factors like attrition or organisational changes lead to instability.

We can help by:

- Establishing a Data Governance council
- Studying business processes and

ORGANISATIONS ARE SLIPPING INTO DATA CHAOS AND BUSINESSES ARE INCREASINGLY MAKING DECISIONS BASED ON GUT INSTINCTS.

sub-processes to identify critical data elements (CDEs). This will help assign most suitable data owner to CDEs.

- c. Working with an organisation's HR in driving change / transformation. Playing the role of data owner effectively should translate into the individual's performance KPI or entered in goal sheet.

Defining and enforcing appropriate data quality rules determine the success of a data quality program. More often than not, data owners are not fully appraised of market regulations, business process fulfillment requirements and the organisation's vision to encompass all dimensions of data quality. Another reason for the failure of DQ programs can be attributed to challenges associated with implementing (coding / programming) rules.

We can help by:

- a. Creating synergies between data stewards, data owners, and data consumers. Data consumers play a crucial role in defining DQ rules, since their analysis is as effective as the quality of data that can impact an organisation's decision-making process.
- b. Identifying CDEs from Organisational KPIs that qualify for enforcing DQ rules. It is important to phase out DQ Implementation programs by way of prioritising CDEs.
- c. Applying regulatory lens, taking into account audit observations while helping data owners define DQ rules.

Remediating data quality defines the final step of any DQ program. Top executives require solutions to problems, and highlighting data quality issues is a mere start. Very often, organisations are misled into investing in new technology applications and spending resources

**MOST ORGANISATIONS
DON'T HAVE VISIBILITY
INTO THEIR DATA,
INCLUDING WHERE THE
DATA RESIDES.**

**SOMETIMES, AN
ORGANISATION SEEKS
QUICK TURNAROUND
SOLUTIONS AND
NOT A MULTI-YEAR
TRANSFORMATIONAL
ROADMAP.**

in migration, for solving DQ issues. Sometimes, an organisation seeks quick turnaround solutions and not a multi-year transformational roadmap.

We can help by:

- a. Creating DQ dashboards with thresholds to only focus on data records that require remediation.
- b. Offering alternate solutions to updating data and creating orphan transactions.
- c. Building a heat map to prioritise CDEs for remediation.

How do you think Privacy impacts organizations moving to the Cloud?

Mohammed Arshad, Managing Director – Cloud Solutions

The rapid development of the cloud has led to more flexibility, cost optimisation, orchestration and scalability of solutions, yet it has also ushered in challenges of privacy and security. Following are some of the key concerns faced by organisations:

- Confidentiality of the user's personal data remains a primary concern when externalising and outsourcing sensitive personal data to the cloud service provider.
- In most public cloud environments, as cloud infrastructure is distributed across different geographical locations, it is often possible that the user's personal data is stored in a location that is outside its legal jurisdiction. This leads to concerns about the legal accessibility of local law enforcement

and regulations on data that are outside the purview of its region. Further, business functions often onboard a SaaS service overlooking some of these geo-restrictions, preferring instead, the ease of service offered.

- Multi-tenancy is a paradigm that follows the concept of sharing technology infrastructure, data storage, applications and services among different tenants. This is then hosted by the same logical or physical platform at the cloud service provider's premises. Attackers can take undue advantage of the multi-residence opportunities and launch various attacks against their co-tenants, resulting in several privacy challenges. Apart from materialising risks pertaining to multi-tenancy, appropriate configurations, if missed out by the provider or the consumer, these can often lead to catastrophic events.

To overcome these concerns, organisations need to adopt a comprehensive privacy program to ensure that the risks are addressed and mitigated appropriately. Following are a few of the measures that organisations can focus on:

- Policies and procedures must explicitly address cloud privacy risks. This should be combined with periodic control design and control effectiveness assessments.
- Data governance must be put in place, that provides tools and procedures for implementing personal data classification and assessing risk in the cloud. It must establish policies for cloud-based processing based on risk and value of assets and evaluate third party security and privacy capabilities before sharing confidential or sensitive personal information.
- Adopt mechanisms such as contractual clauses, to protect data sharing/data localisation requirements with cloud service providers and avoid risks such as vendor lock in, non-compliance, etc.
- Privacy must be managed thorough review and audit of providers and independent third- party verifications, to ensure that providers have appropriate controls in place. **i**

RESECURITY IDENTIFIES INVESTMENT SCAM NETWORK “DIGITAL SMOKE”

Resecurity identified one of the largest investment fraud networks by size and volume of operations created to defraud Internet users from Australia, Canada, China, Colombia, European Union, India, Singapore, Malaysia, United Arab Emirates, Saudi Arabia, Mexico, the U.S. and other regions. The bad actors operating as an organized crime syndicate developed a massive infrastructure to impersonate popular Fortune 100 corporations from the U.S and the U.K by using their brands and market reputation to defraud consumers. Once payments are collected from the victims, they make previously created resources vanish and set up the next new campaign - this is why investigators named the group “Digital Smoke”.

According to the latest report by FTC released last week called “The Top Scams of 2022” people reported losing \$8.8 billion to scams. The total damage from investment fraud including ponzi and pyramid schemes exceeds \$5.8 billion in the U.S and over \$77 worldwide (2022), with significant rapid growth at the start of Q1 2023. Investment fraud does serious damage to investors – beyond monetary losses. A FINRA survey points to health, marital and

trust problems resulting from financial scams. Businesses experience significant damage in customer loyalty and brand reputation - in the long run negatively affecting sales and market profile.

Notably, the bad actors have chosen high-demand investment areas to impersonate world-known brands including ABRDN (UK), Blackrock (US), Baxter Medical (US), EvGo (US), Ferrari (Italy), ITC Hotels (India), Eaton Corporation (US/UK), Novuna Business Finance (UK), Tata (India), Valesto Oil (Malaysia), Lloyds Bank (UK), and many more. The majority of the identified fraudulent projects were related to financial services (FIs), oil & gas, renewable energy, EV batteries, electric vehicles, healthcare, semiconductors, and world-recognized investment corporations and funds with a global presence.

The information about Digital Smoke along with the identities of key actors has been timely shared with the Indian Cybercrime Coordination Center and the U.S. Law Enforcement in Q4 of 2022. In

the result of the coordinated action and numerous domain takedowns, the majority of scam projects have been terminated.

The modus operandi of the group was focused on investment options in non-existing products and investment plans supposedly offered by the Fortune 100 corporations and state-owned entities. The bad actors developed a large network of WEB-resources and related mobile applications hosted on bulletproof hosting providers, and located in jurisdictions not easily reachable for immediate takedowns – the total number of identified hosts in December 2022 alone exceeded 350+ with thousands of related domains used for ‘cloaking’ (Black SEO), hidden redirects and short URLs for protection of the payment gateway used by fraudsters to collect payments from victims leveraging AliPay (China) and Unified Payments Interface (UPI) - an instant real-time payment system developed by National Payments Corporation of India, along with cryptocurrencies. Notably, a combination of these methods enabled fraudsters

DIGITAL SMOKE HAS CLEARLY DEMONSTRATED HOW BAD ACTORS LEVERAGE CROSS-BORDER PAYMENTS AND VARIOUS JURISDICTIONS TO COMPLICATE FURTHER INVESTIGATION AND IDENTIFICATION OF THEIR VICTIMS.



to process funds with great flexibility – supporting Google Pay (GPay), PhonePe, Paytm, and major online-banking platforms.

The bad actors registered multiple fake domain names which had similar brand spelling then promoted them via social media and instant messenger apps to attract investors. Notably, the links planted by bad actors to register new victims contained a referral code tied to affiliates promoting the scam via Youtube and Whatsup IM. Once the victim registers, the bad actors ask them to make a deposit by sending payment to an account registered in India.

Notably, the cybercriminals from Digital Smoke were focused on oil markets and renewable energy products. The impersonated Velesto Oil, a Malaysia-based multinational provider of drilling for the upstream sector of the oil and gas industry, along with major oil corporations including Shell, Glencore, Orintiv and Lukoil. One of the latest brands abused in January 2023 was identified as ACWA Power based in the Kingdom of Saudi Arabia.

This aspect makes the campaign unique due to a strong focus on oil traders which typically is not widely used by investment scammers. In some of the observed scams, the bad actors offered victims the opportunity to invest in new oil fields, construction of petroleum stations, and technologies related to the renewable energy sector. It's worth noting, some of the language for this pretext was copied from existing investment programs, typically for entrepreneurs and franchises looking for new business opportunities in the oil and gas sector. This activity is not typical for cybercriminals and may clearly outline the differentiator of the Digital Smoke group. The activity spike was registered during the Christmas and New Year's period, when online activity skyrocketed, and when both Internet users and financial institutions get overwhelmed with logistics and payments. In Q1, 2023 – the activity continued to involve new impersonated brands from other fields including semiconductors and EV batteries.



Besides enterprises, the fraudsters had no fear when it came to targeting state-owned organizations and used their profiles to defraud users. One of the organisations impersonated by the Digital Smoke fraudsters was the India Brand Equity Foundation, a Trust established by the Government of India - Department of Commerce, Ministry of Commerce and Industry. Following a similar pattern, the bad actors created multiple scams which impersonated government resources in United Arab Emirates by copying the profile of the Minister of State for Foreign Trade.

The Digital Smoke case is somewhat remarkable and may confirm how investment scams have now become more sophisticated than before. Fraudsters are investing large amounts of time and effort to prepare high-quality resources which look almost identical to their well-known investment product counterparts - in the case of Digital Smoke, for each investment scam they ran, they also created a separate mobile app with a unique design.

Digital Smoke has clearly demonstrated how bad actors leverage cross-border payments and various jurisdictions to complicate further investigation and identification of their victims. The investment fraudsters

leverage this weakness to blur the origin of the activity as well as distribute payment flows by multiple merchants and money mules located in different countries. Resecurity identified a large network of money mules leveraging accounts in multiple financial institutions based in India who process the payments from victims. The accounts involved in fraudulent activity have been reported to law enforcement.

"Proactive fraud intelligence gathering enables to protect consumers and keep financial institutions aware about merchants used by cybercriminals. Their timely identification along with tracking of involved money mules helps to minimize potential damage caused by illicit activity," said Christian Lees, Chief Technology Officer (CTO) at Resecurity, Inc.

Notably, legitimate businesses who were impersonated suffer serious damages, both reputationally and from a customer loyalty perspective - that's why an effective and ongoing brand protection system is one of the must-have solutions to minimise the negative side effects of such scams. Business leaders should consider monitoring the exposure of their brands online including but not limited to social media, mobile marketplaces, and instant messaging services. 🔑

Solar Powered Camera

No network cable required

Powered by solar energy, this kit sets up without any electrical wiring.

Easy installation

Easy set up without mechanical equipment-reducing the installation costs and time.

Can withstand bad weather

Prone to extreme weather such as strong wind and rainstorms.



2MP
@ 30 fps



40W



20 Ah
lithium



4G



Beaufort
scale **12**



IP67



Scan to Learn More



HIKVISIONMENA



HIKVISION-MENA



HIKVISIONMENA



HIKVISIONMENA

HIKVISION

WOMEN IN SECURITY

MARCH IS THE MONTH CELEBRATING WOMEN AND THEIR ACHIEVEMENTS. ON THIS OCCASION, WE SPOTLIGHT SOME OF THE LEADING LIGHTS IN CYBERSECURITY.



AREEJ ESSA, SENIOR ASSOCIATE, INFRASTRUCTURE SPECIALIST, KYNDRYL

I work as a senior associate specialising in infrastructure, where I work with customers on a daily basis to advise them on their most secure journey to the Cloud. This means that I have to understand their needs and advise them on the most secure, cost-effective, and reliable solutions.

Part of my job is also to implement their cloud solutions in their space to support their business. Since the infrastructure we build runs the applications, security is one of the most important aspects to consider in my day-to-day work. I study the security considerations from the perspective of the infrastructure, applications, network, and access management of the environment and ensure the solution addresses each of them.

I believe that security is a very fast and wild field that combines many technologies. When you work in security, you always have to be prepared for unexpected situations. I do enjoy that state of readiness that one must constantly be in and being a step ahead of increasingly uncertain times.

The first thing that comes to mind is this quote: "we may have all come on different ships, but we are in the same boat now". When I face challenges at work, I turn to my team, who support me in solving the problems without hesitation, and I'm grateful to be working with them.



ALAINA HUYSAMEN, MARKETING MANAGER FOR AFRICA , KASPERSKY

I work closely with our channel partners and sales team to create a more sustainable model for marketing and customer engagement. This means reinventing and tailoring systems and processes to create a more efficient and dynamic team.

"I'm driven by the fact that this is a people-oriented job and provides me with ample opportunities for self-education. Discovering a whole new world of cybersecurity and cybercrime and planning focused marketing strategies for the betterment and protection of our customers keeps me motivated.

I think my job represents an opportunity to make a difference, and this motivates me every day. I firmly believe that my team and I can help break gender bias through the work we do. For example, our campaigns, activations, webinars and training programs are designed to raise awareness about having female leaders in the cybersecurity industry, and educate female students on the possibility of having a career in cybersecurity.

Kaspersky has put words into action when it comes to building an inclusive and diverse workplace. Treating difference of opinion, perspective and skills as a strength is one of the many things that has worked for me. "

**CHARLINE FAHED, FIELD MARKETING
MANAGER, META, SENTINELONE**

As the Senior Marketing Manager for Middle East, Africa and Turkey, I oversee multiple responsibilities to drive sales and brand awareness. This includes organising field events, managing marketing plans, and generating leads to meet pipeline targets. I also work closely with the sales team to identify target markets and use executive contacts to support sales with client meetings via direct engagement and marketing activities. Other responsibilities include developing brand awareness activities through local media, analyst and consultant relationships, working with channel partners and distributors on all marketing initiatives and execution, and engaging with tele-sales to ensure proper dialogues and support promotional preparations with the BDR team. Finally, I push my colleagues to play their roles as part of a united team to ensure that we all work together to achieve our goals.

"I've always had a strong interest in staying up to date with the latest technologies and security threats. I believe that security is a crucial aspect of any technology-related field, as without proper security measures in place, all other technological advancements are at risk. This belief has driven me to work in the security field, where I am constantly challenged to stay ahead of ever-evolving threats, while having the opportunity to work with cutting-edge technology. Being a part of this dynamic industry, where every day brings new challenges, is truly exhilarating and fulfilling.

To solve marketing challenges effectively, I follow a structured approach: defining the problem, researching and gathering information, developing a detailed plan, collaborating with colleagues in other departments, such as product development or sales and channel, iterating and testing, and staying adaptable. This approach



enables me to make informed decisions, use data and feedback to adjust my strategies, and stay open to new opportunities in a constantly evolving marketing landscape. By following this approach, I can effectively address marketing challenges and drive business success."

**DANIELLE JABLANSKI, OT CYBERSECURITY
STRATEGIST, NOZOMI NETWORKS**

As an OT cybersecurity strategist at Nozomi Networks, I am responsible for researching global cybersecurity topics and promoting operational technology (OT) and industrial control systems (ICS) cybersecurity awareness throughout the industry. I also represent Nozomi Networks at the OTCC, ISAGCA, ISAC communities and more government relations.

While securing critical infrastructure inspires me, the consistent problem-solving, community-building and teamwork motivate me in this industry – because technology is everchanging. What's built, innovated, scrapped, and connected continues to evolve at a pace that once seemed impossible. Despite this pace, there are still many problems to solve. Processes and people are still the most important factors. While there is no perfect answer, and no solution fixes everything, there is excitement in finding alternatives, and new answers.

I'm lucky to have found many champions in this industry, both men and women alike. Throughout my career, I've dealt with negative biases regarding gender, age, and seniority. Instead of fixating on them, however, I nourish the professional relationships I have with mentors I respect, and whose respect I have earned intellectually from the start.

You should never have to prove to anyone that you belong at the table you are already sitting at. Don't waste time getting the work done – you're there to do a job you are qualified to do, and no one can take that away from you.

JULIE DAVILA, VP OF GLOBAL FIELD CTO OPERATIONS, SOPHOS

My work primarily focuses on building a team that serves as a force multiplier to our cybersecurity vision with concentrated attention to enterprise needs within specific focus areas (like the public sector). Within Sophos, I lead the global field CTO team, a highly-experienced group of executive-level ambassadors, who are also accomplished researchers, innovators, entrepreneurs, and spokespeople who possess and demonstrate expertise in their domains. For my role, I am the “field CTO for the public sector,” so I focus on most of my work on government and education.

There are different types of challenges. They are typically either challenges regarding insufficient knowledge or constraints. In both cases, the options are to reduce the impact of the challenge, remove the challenge altogether, or work through the challenge. Regardless of the preferred option, it’s always important to me to ensure a fast feedback loop regarding the approach I decide to take. These feedback loops tell me whether or not I should address the challenge differently based on observable facts. My common approach to this system is by formulating a hypothesis: “Given what I know to be true, I will attempt Y-approach,” where the approach is developed independently or with a team. Then, an equally important part of that hypothesis is defining indicators of success and failure. What does it look like for Y-approach to have succeeded? What are the failure indicators? The idea is to make it easy to try the next hypothesis without falling victim to sunk costs or other traps. This approach allows me to address challenges in my work effectively.



LINA RAMADAN, FIELD MARKETING MANAGER, INFOBLOX

As Field Marketing Manager at Infoblox, my focus is on the Middle East, Africa, Turkey, and Pakistan regions. I am responsible for overseeing all marketing efforts that extend beyond digital channels, including social media, educational programs, and networking experiences. Additionally, I am particularly passionate about account-based marketing and enjoy working on content creation. Overall, my role involves managing diverse marketing activities and ensuring they align with the company’s goals and objectives.

One of the primary things that excites and motivates me about my job is my team. I enjoy human interactions and find it incredibly fulfilling to work with others towards a common goal. Additionally, I firmly believe that cybersecurity is everyone’s responsibility and that all investments, including human resources and funds, coupled with awareness, are critical for the greater good of humanity. As the saying goes, “safety-first.” Being able to contribute to such an important cause and work alongside talented and passionate colleagues is what motivates me every day.

I do love me a good challenge! I usually tend to calm myself down in order to think with a clear head, then break down the challenge and seek advice from colleagues and mentors. I explore solutions and take calculated risks while remaining adaptable and open to change. It is very important to surround yourself with good, smart people, because ultimately, working as a team in order to tackle challenges is key to success.

NATHALIE RIVAT, VP OF SYSTEM ENGINEERING , FORTINET

I lead a team of Consultant Systems Engineers (CSEs). This has been a fantastic role as I'm at the crossroads of sales, pre-sales, product management, engineering and training teams and am exposed to different areas of the business. My team helps shape the development of product lines based on customer feedback. CSEs play a key role in product evolution as they work with engineering, reporting what customers and prospects require and how our products can best meet those needs. Building a flexible team that can onboard any technology and product line is not easy. I'm proud of all the contributions my team makes to such a large part of Fortinet's business.

It's fascinating to see the early days of new product lines and be responsible to onboard teams in a sales territory, identifying where to sell and how to sell. It is even more exciting to have this role in a company that has kept the agility it demonstrated in its early days, continuing to accelerate its innovations in various product areas.

Being a woman in cybersecurity in a technical role is breaking the stereotype. I never accepted to let stereotypes decide what my life should look like and what I should do for a living. I hope that my own career path helps inspire other women to pursue a senior management position in cybersecurity and not be intimidated to take the first step, whether they are just starting their careers or have been in the workforce for years.



NEVINE EL TANAHY, ALPHA DATA

I lead marketing in Alpha data for UAE, Saudi and Qatar.

I enjoy the fact that regardless of whether we are working on a campaign, organising events, or engaging in any other activities, I always approach them with the same level of enthusiasm and apprehension as if it were my first campaign. I am driven by the desire to ensure that we execute everything flawlessly, just as if it were our initial undertaking.

It's my firm belief that every challenge we encounter presents an opportunity for us to find a solution. To resolve any issues effectively, we must take a step back and consider the entire situation in its entirety, rather than focusing solely on individual components. In doing so, we can avoid playing the blame game and instead work collaboratively to develop practical solutions that address the root cause of the problem.

Finding joy in what you do is crucial, and it's also essential to collaborate with reliable individuals who can help you advance to the next level. In my opinion, what sets women apart is their ability to balance emotion and logic, which enables them to approach challenges with a unique perspective. This blend of qualities allows women to approach problems with empathy while still being rational and objective. By combining these two attributes, women can make a meaningful impact in their respective fields, providing solutions that are not only effective but also empathetic and compassionate.

NICHOLA BANERJEE, REGIONAL MARKETING MANAGER – META & CEE, BARRACUDA

As a marketer, my role involves developing plans and strategies that are closely aligned with the overall goals of the company. To achieve this, I work closely with the channel, sales, and pre-sales teams to ensure that our marketing initiatives are effective and impactful. One of my key responsibilities is developing, implementing, and executing marketing activities that make the best use of our budget. Additionally, I liaise with our distributors and partners to ensure that our campaigns are executed effectively and efficiently.

I find the security industry to be an incredibly exciting and constantly evolving field which is what enticed me to be a part of it. The fast pace and ever-changing nature of the industry provide a sense of challenge and excitement that keeps me constantly engaged in my work.

While marketing for the technology industry can be challenging, I find that seeing the impact of my work not only on the growth and success of my organisations, but in the ability for end customers to embrace digital transformation, incredibly rewarding. Watching my organisation grow through the implementation of successful marketing strategies gives me a great sense of accomplishment and satisfaction.

Marketing for a technology company means constantly evolving to staying ahead of the curve and keep up with the latest trends. The technology industry is one that demands individuals to have a passion for learning and a desire to adapt to change. With technology advancing at a rapid pace, I find the skills required in marketing are also shifting. Therefore, I remain open to learning new things and constantly upskilling.



WASNA BENGASSEM, REGIONAL MARKETING DIRECTOR, TREND MICRO MEA

As the Regional Marketing Director for Trend Micro Middle East & Africa, I am responsible for elevating the company's brand and mission to make the world safer for exchanging digital information by engaging customers, partners, media, and other stakeholders.

I was drawn to the field of cybersecurity because it combines my passion for technology with the opportunity to make a real impact in protecting our communities and organizations from cyber threats. It's an ever-evolving field that requires constant learning and adaptation, which keeps me motivated and engaged.

Being part of a global company like Trend Micro that is at the forefront of cybersecurity innovation, and working alongside a talented team, has only reinforced my passion for the industry. I am proud to be a part of this dynamic and vital field and to contribute to making the world a safer place.

To overcome challenges in my role, I prioritise staying ahead of the curve, collaborating and leveraging data and insights to develop effective solutions, and remaining flexible and adaptable to pivot strategies as needed.

ADVERSARIES CAN SPOT YOUR SILLY MISTAKES

■ SATYKAM ACHARYA, DIRECTOR RED TEAM, INFOPERCEPT CONSULTING PVT LTD

English grammar is a comprehensive subject, and we all have faced a strict grammar teacher at some point in our lives. The typical attribute of a strict grammar teacher is that he or she is well trained in pointing out silly mistakes.

One thing that is common between adversaries and a grammar teacher is their eye for detail which helps them find errors which otherwise go unnoticed. While the silly mistakes found by our grammar teacher are better for our careers, they can be lethal if found by adversaries in the cyber world. Adversaries capitalize on silly mistakes found in the entire IT landscape and establish a foothold in any network they want and then do lateral movement to launch a sophisticated cyberattack.

At Infopercept, offensive security is one of our main offerings. Offensive security is a field of cybersecurity, which focuses on security testing

and training. Its main goal is to help organizations improve their cybersecurity posture by identifying vulnerabilities and weaknesses in their systems through ethical hacking and penetration testing.

While leading Infopercept's offensive security, I have been lucky to act and think like an adversary, but for the improvement and benefit of the overall cybersecurity posture of our clients. Working on many such assignments, we have realized that organizations often make silly mistakes in their cybersecurity, which attract adversaries.

Hardcoded Credentials in Applications:

While doing penetration testing for one of the largest banks in Mongolia, we started our task with downloading their internet banking mobile app from the play store. Penetration testing is an exercise where our clients invite us to break their systems to check for vulnerabilities. Under this particular project, we were not given any information other than publicly available entities like their apps and website.

After downloading the app, we decompiled the APK file. When any application is developed, the original source code is compiled in the Android Packaged Kit (APK) file, a binary file, which runs on an Android Device. Decompiling an APK file means we reverse engineer it to extract its original source code. There are tools called 'decompilers' through which this can be done very easily.

To our surprise, we found hardcoded credentials in the APK file. Through these credentials, we were able to login into the app and were able to download other user's statements. This was just the initial foothold we needed, after which we could do many things with these credentials.

Hardcoded credentials are the silliest security mistakes one can make. It refers to login credentials of the application embedded in the software program's code itself. The best example to understand this is like having your ATM sim cards pin written on the card itself. If someone has access to your card, they can exploit it as you have written your pin on the card itself.

To avoid this mistake, security should be followed as a best practice from the coding stage itself. Developers should store the credentials securely by using methods like encryption and password hashing.

HARDCODED CREDENTIALS ARE THE SILLIEST SECURITY MISTAKES ONE CAN MAKE. IT REFERS TO LOGIN CREDENTIALS OF THE APPLICATION EMBEDDED IN THE SOFTWARE PROGRAM'S CODE ITSELF.

Not Masking Credit Card Details Throughout:

During our exercise with the same client, we found that they were not masking credit card information throughout their environment. Masking refers to making sensitive information like credit card number, expiration date, and security code, not readable or understandable.

Masking is the minimum best practice that a financial institute should exercise. However, the institute was not doing it throughout. And because of it we were able to successfully use bruteforce (a trial-and-error method to get perfect details from the details available) and print credit card statements.

Core Applications Code Available Publicly:

Offensive security is often practiced by Fintechs, and one of the largest fintechs from the Middle East approached us to do a red teaming exercise for them. Red teaming is an exercise where they hire us to do actual attacks on their systems and help them discover vulnerabilities in their people, processes, and technologies.

We could easily download the entire source code of their application, as it was publicly available on their website. This was the worst place to have such information. We simply visited their website and downloaded their entire source code of applications without any authentication.

From that source code, we were able to get admin credentials, logged into the application, and got access to their database which led us to their Personally Identifiable Data. This was akin to getting the keys to open any lock in the organization. We made them realize the amount of damage this silly mistake would have cost them, if the information had been accessed by real adversaries.

Just like in grammar, in order to avoid silly mistakes, we need to practice consistently. Organizations should have an offensive first and offensive daily approach to find their silly mistakes. It is better that a red teamer finds your silly mistakes than an adversary. 🗝





Celebrating **WOMEN POWER IN TECHNOLOGY**



Women currently make up over 25% of the global technology workforce and according to official estimates, this number is growing fast. The varied experiences of women in this field, the diversity in their roles with their experience demonstrating a range of skills such as people management, team building, communications and technology consulting, was the focus of the Women in Tech (Pride of Tech) conference and awards. While the awards aimed to enhance the visibility of women in the technology space, recognise their outstanding contributions and enable the next generation of women to aspire for it, the forum and panel highlighted the exceptional efforts made by women to break digital boundaries and create a more inclusive global workforce. This year, the focus was on growth, continuity and results driven by women—particularly how they’ve emerged stronger despite the socio-economic challenges over the past two years.

INFLUENTIAL SALES PERSONALITY
OF THE YEAR



NIGINA BENDER

JABRA

TRAILBLAZER OF THE YEAR



SELINA BIEBER

GODADDY

TECHNOLOGY EXECUTIVE LEADER
OF THE YEAR



HAIDI NOSSAIR

DELL TECHNOLOGIES

TECHNOLOGY VISIONARY
OF THE YEAR



LOUBNA IMENCHAL

LOGITECH



tahawultech.com

Women
in
TECHNOLOGY
FORUM AND AWARDS
2023

TECHNOLOGY BUSINESS LEADER
OF THE YEAR - GOVERNMENT



SHEEBA HASNAIN

SHARJAH DOCUMENT DEPARTMENT

MARKETING INNOVATION LEADER
OF THE YEAR



MARY KOKAIA

DU BUSINESS

CHANNEL CHIEF OF THE YEAR



EKTA PUTHRAN

BARCO

MARKETING EXECUTIVE
OF THE YEAR



SOUSSANE CHARTOUNY

PALO ALTO NETWORKS

 **tahawultech.com**

Women in TECHNOLOGY FORUM AND AWARDS 2023



MARKETING EXECUTIVE
OF THE YEAR



LANIA HANNOUSH

DELL TECHNOLOGIES

MARKETING EXECUTIVE
OF THE YEAR



YASMIN KHALIQ

EQUINIX

BRAND STRATEGIST OF THE YEAR



SHAED KHADER

LOGICOM DISTRIBUTION



tahawultech.com

Women
in
TECHNOLOGY
FORUM AND AWARDS
2023

BRAND STRATEGIST OF THE YEAR



USHA GOOLAPPA

IFS

BRAND STRATEGIST OF THE YEAR



AMRITA CHANTY

GULF IT NETWORK DISTRIBUTION

WOMAN EXECUTIVE OF THE YEAR



MAYA ZAKHOUR

NETAPP

MARKETING TRANSFORMATION
PIONEER OF THE YEAR



NAGHAM HALABI

VEEAM SOFTWARE

CHANNEL MARKETING STRATEGIST
OF THE YEAR



TARANNUM SAQIB

INGRAM MICRO

tahawultech.com

Women in TECHNOLOGY FORUM AND AWARDS 2023



STRATEGIC SALES LEADER
OF THE YEAR



KONICA KHANDELWAL DHAWAN

BEST TECHNICAL CONSULTANT
PERSONALITY OF THE YEAR



ANAM IQBAL

MARKETING RISING STAR
OF THE YEAR



ASHA PRAKASH

SEIDOR MENA

MALCO TECHNOLOGIES

MARKETING RISING STAR
OF THE YEAR



TAHAWULTECH.COM

Women
in
TECHNOLOGY
FORUM AND AWARDS
2023



GHADAH HUMADI

ALTERYX

MARKETING RISING STAR
OF THE YEAR



SIRIN AKROUK

PURE STORAGE

INFLUENTIAL MARKETING
PERSONALITY OF THE YEAR



SANDY ISSA

INTELLIGENT SECURITY SYSTEMS

TECHNOLOGY BUSINESSWOMAN
OF THE YEAR



SHERIFA HADY

HPE ARUBA NETWORKING

SENIOR MARKETING LEADER
OF THE YEAR



CHANTELLE TAVID

NVIDIA

 **tahawultech.com**

Women
in
TECHNOLOGY
FORUM AND AWARDS
2023





**SENIOR MARKETING LEADER
OF THE YEAR**

**TECHNOLOGY INNOVATOR
OF THE YEAR**

**CHANNEL SALES LEADER
OF THE YEAR**



RAJI JOY JOHN

STARLINK



REENA ALEX JOHN

FINESSE



SEEMA WADHWA

EXCLUSIVE NETWORKS



MARKETING PERSONALITY
OF THE YEAR



NICHOLA BANERJEE

BARRACUDA NETWORKS

MARKETING PERSONALITY
OF THE YEAR



WIDAD ABDALHADHI

CISCO

SENIOR MARKETING LEADER
OF THE YEAR



VARUNA SHAH

MINDWARE

SENIOR SALES LEADER
OF THE YEAR



ANITA QUADROS

ANIXTER

 **tahawultech.com**

Women
in
TECHNOLOGY
FORUM AND AWARDS
2023



INNOVATIVE TECHNOLOGY MARKETING
PERSONALITY OF THE YEAR



YARA MILBES

CEQUENS

BRAND AWARENESS
MARKETEER OF THE YEAR



ZAHRA HANIF

THALES GROUP

BRAND AWARENESS MARKETEER
OF THE YEAR



KIARA ISRANI

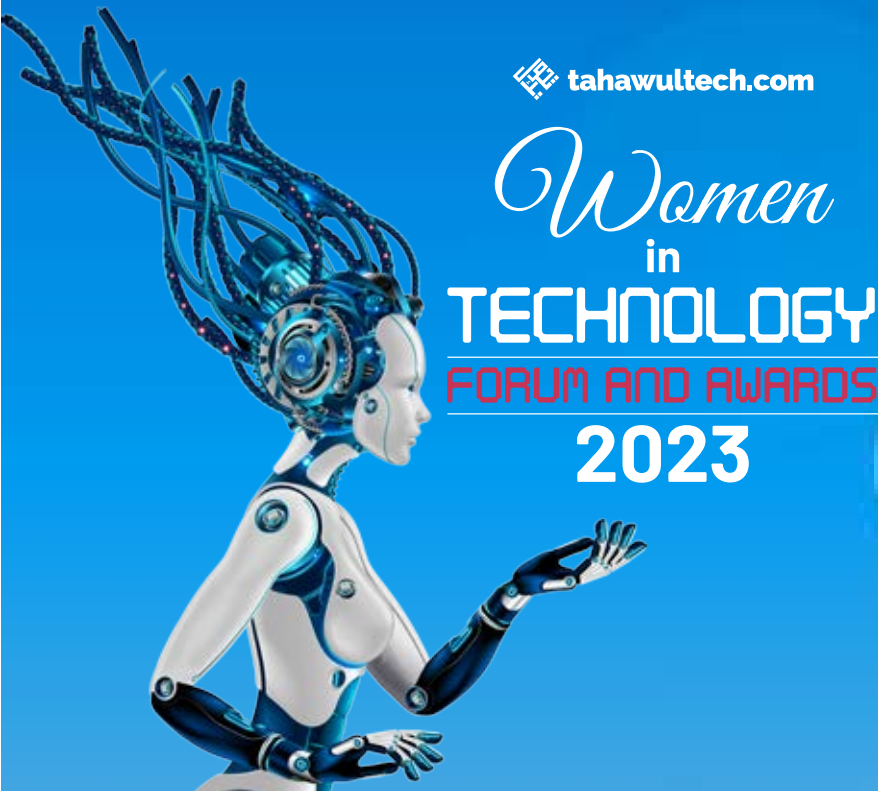
SECUREWORKS

BRAND AWARENESS MARKETEER
OF THE YEAR



GUNIKA ARORA

QUEST SOFTWARE





**MARKETING TRENDSETTER
OF THE YEAR**



BINDHYA RAMADASA
FORESCOUT TECHNOLOGIES

**MARKETING TRENDSETTER
OF THE YEAR**



APARNA CHATURVEDI
NEWCOM COMPUTER SYSTEMS LLC

**MARKETING TRENDSETTER
OF THE YEAR**



RIDDHI ANILKUMAR
ACRONIS



**INSPIRATIONAL WOMAN
LEADER 2023**



MAREVA KOULAMALLAH

**INSPIRATIONAL WOMAN
LEADER 2023**



NADINE CHAMMAS

**INSPIRATIONAL WOMAN
LEADER 2023**



FATIMA AL QUBAIS

MARKETING EXECUTIVE OF THE YEAR
MANAL ABI RAFEH FORTINET

BRAND STRATEGIST OF THE YEAR
NOURA SHIHABI TREND MICRO

SENIOR MARKETING LEADER OF THE YEAR
NILU KAMKARFAR RACKSPACE TECHNOLOGY

BRAND STRATEGIST OF THE YEAR
RASHA ISLIM EMITAC ENTERPRISE SOLUTIONS

MARKETING PIONEER OF THE YEAR
LENA HALBOURIAN COMMVault

MARKETING PERSONALITY OF THE YEAR
RAANIA AL KHATIB JUNIPER NETWORKS

MARKETING PERSONALITY OF THE YEAR
RASHMI PURSWANI BENQ

**GOVERNMENT PERSONALITY OF THE YEAR -
STRATEGY AND GROWTH**
MARIAM S. MUBARAK ABU DHABI PORTS GROUP

TECHNOLOGY BUSINESS LEADER OF THE YEAR
SIMRAN BAGGA OMNIX INTERNATIONAL

BRAND AWARENESS MARKETEER OF THE YEAR
SHAFIYA SAMREEN RAQMIYAT

SENIOR MARKETING LEADER OF THE YEAR
MALLIKA SHARMA HPE ARUBA NETWORKING

MARKETING TRENDSETTER OF THE YEAR
SUMAIYA MUHAMMAD MITEL

INSPIRATIONAL WOMAN LEADER 2023
FAZEELA GOPALANI

MARKETING TRENDSETTER OF THE YEAR
ANKITA JAVERI GBM

BRAND AWARENESS MARKETEER OF THE YEAR
SANCHARI ROY BARCO

INSPIRATIONAL WOMAN LEADER 2023
LEILA SERHAN



www.gulfitd.com

The *Fastest* Growing **VAD**

imperva

PingIdentity.

NIAGARA
NETWORKS

Array

CATO
NETWORKS

PENTERA

CYBLE

netwrix

RESOLVE

aruba

SailPoint

CYBERARK

sealpath.

corelight

Fortanix

IT'S TIME TO CREATE MORE OPPORTUNITIES FOR WOMEN IN CYBERSECURITY

■ RENÉE TARUN - DEPUTY CISO / VICE PRESIDENT INFORMATION SECURITY

Undoubtedly, our industry needs to create more initiatives to attract a more diverse group of professionals, including women, to STEM-focused careers like cybersecurity. While we've collectively made some progress on this front, a great deal of work still needs to be done to bring women into cybersecurity-focused roles and create meaningful career paths for them to grow and progress within the industry.

While women make up nearly 50% of the world's population, they only account for an estimated 24% of the cybersecurity workforce. At the same time, the cybersecurity skills gap remains dangerously high, and the volume of cyberattacks impacting organizations of all shapes and sizes is growing every day.

As we celebrate International Women's Month this March, we're reminded that there's much more that can and should be done to create opportunities for women to grow or jump-start a career in cybersecurity.

The Many Benefits of Building More Diverse Teams

A wealth of data demonstrates just how valuable women are to the overall workforce. For example, studies show that women bring crucial soft skills to the workplace regardless of what industry they're in and often outperform men in areas such as taking initiative, communicating, demonstrating

resilience, building relationships, and developing others.

Organisations that successfully build more diverse teams experience a variety of benefits. Not only is diversity good for an enterprise's bottom line, but it also cultivates increased creativity and innovation and lays the foundation for better problem-solving and decision-making. Additionally, diverse companies are 70% more likely to capture new markets and 120% more likely to achieve financial goals.

Three Ways to Create More Opportunities for Women in Cybersecurity

In 2021, 53% of Americans quit their jobs in pursuit of a career change, and experts witnessed the "Great Resignation" continuing well into 2022. With so many professionals currently looking to explore opportunities in new industries, there's no better time for the cybersecurity industry to implement unique programs to draw new talent, particularly those from underrepresented groups, like women, to the field.

Here are several ideas on how to attract more women to cybersecurity roles.

Develop Training and Upskilling Opportunities

Offering hands-on training and upskilling opportunities is a great way to attract new talent to the cybersecurity industry, giving learners a chance to kickstart a new career by learning cybersecurity fundamentals in a low-pressure environment. These offerings can also

support women who already work in cybersecurity but want to grow and advance in their careers.

The Fortinet Training Institute partners with several organisations focused on advancing women in security, including WiCyS and Latinas in Cyber, to provide their members with access to Fortinet's industry-leading training and certification curriculum. Fortinet also partners with Cyversity to offer free and discounted cybersecurity training to women and underrepresented minorities interested in pursuing a career in the industry.

Offer Internships

While internships are often viewed as reserved for students or recent graduates, internship opportunities also offer career changers valuable hands-on experience in a new industry. Internships can be a great starting point for women interested in working in cybersecurity, and these roles typically provide chances for mentorship and networking.

Numerous organisations focus on connecting women of all career levels with STEM- and cybersecurity-focused internship opportunities. One example is WiCyS, which offers a single internship application process that connects applicants with engaged employers actively seeking internship candidates.

Implement Mentorship Programs

Mentorship programs are a powerful tool for increasing the number of women in cybersecurity, as well as retaining them. These offerings also play a role in

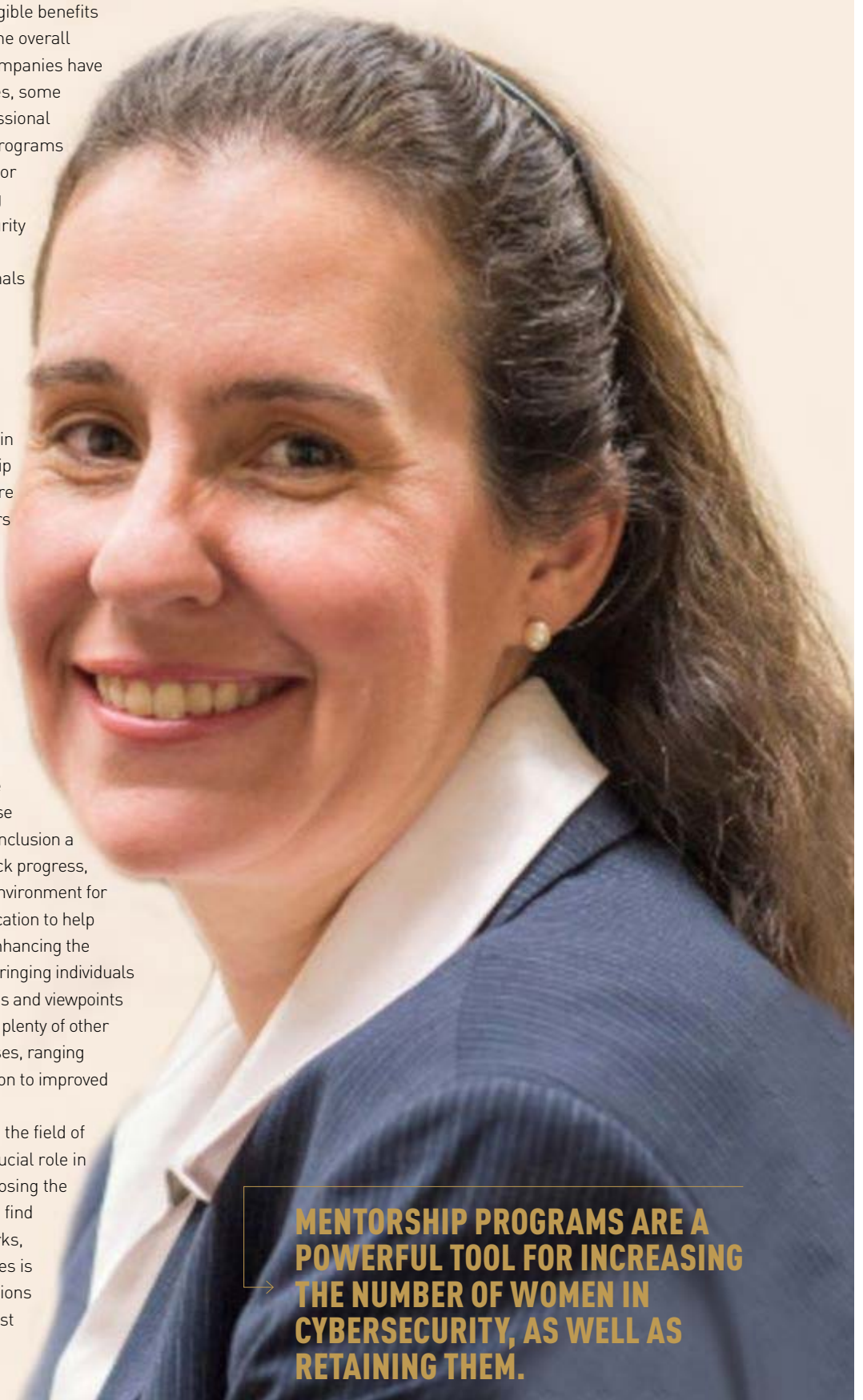
building and advancing a culture of inclusion at any organisation, with tangible benefits for mentors, mentees, and the overall organisation. While many companies have internal mentorship initiatives, some cybersecurity-focused professional organisations offer similar programs that are particularly helpful for women who are still working toward a full-time cybersecurity role or wish to develop relationships with professionals in the broader industry.

For example, an in-depth case study of a mentorship program at a technology company shows that employees who participated in the organisation's mentorship program were five times more likely to advance their careers than non-participants, and mentors achieved similar progress.

Cultivating a Culture of Inclusion

Public and private sector organisations need to create initiatives with the goal of attracting and retaining more women in cybersecurity. These organisations need to make inclusion a priority and measure and track progress, train leaders and create an environment for open dialogue and communication to help make this happen. Beyond enhancing the diversity of the industry and bringing individuals with more varied backgrounds and viewpoints into the profession, there are plenty of other tangible benefits for businesses, ranging from better employee retention to improved financial results.

Attracting more women to the field of cybersecurity also plays a crucial role in filling important roles and closing the skills gap. As cybercriminals find new ways to infiltrate networks, filling open cybersecurity roles is table stakes for all organisations as they work to defend against increasingly complex cyber threats. 🗡️



MENTORSHIP PROGRAMS ARE A POWERFUL TOOL FOR INCREASING THE NUMBER OF WOMEN IN CYBERSECURITY, AS WELL AS RETAINING THEM.

KNOWN VULNERABILITIES POSE GREATEST THREAT TO ORGANISATIONAL SECURITY: TENABLE RESEARCH

Tenable, the Exposure Management company, released its annual 2022 Threat Landscape Report, which validates the persistent threat posed by known vulnerabilities – those for which patches have already been made available – as the primary vehicle for cyberattacks. The findings are based on the Tenable Research team's analysis of cybersecurity events, vulnerabilities and trends throughout 2022, including an analysis of 1,335 data breach incidents publicly disclosed between November 2021 and October 2022.

The Tenable Threat Landscape Report categorises important vulnerability data and analyses attacker behavior to help organisations inform their security programs and prioritise security efforts to focus on areas of greatest risk and disrupt attack paths, ultimately reducing exposure to cyber incidents. Of the events analysed, more than 2.29 billion records were exposed, which accounted for 257 Terabytes of data. More than 3% of all data breaches identified were caused by unsecured databases, accounting for leaks of over 800 million records.

Threat actors continue to find success with known and proven exploitable vulnerabilities that organisations have failed to patch or remediate successfully. According to the Tenable report, the number one group of most-frequently exploited vulnerabilities represents



a large pool of known vulnerabilities, some of which were originally disclosed as far back as 2017. Organisations that failed to apply vendor patches for these vulnerabilities were at increased risk of attacks throughout 2022.

The top exploited vulnerabilities within this group include several high-severity flaws in Microsoft Exchange, Zoho ManageEngine products and virtual private network solutions from Fortinet, Citrix and Pulse Secure. For the other four most commonly exploited vulnerabilities – including Log4Shell;

Follina; an Atlassian Confluence Server and Data Center flaw; and ProxyShell – patches and mitigations were highly publicised and readily available. In fact, four of the first five zero-day vulnerabilities exploited in the wild in 2022 were disclosed to the public on the same day the vendor released patches and actionable mitigation guidance.

"The data highlights that long-known vulnerabilities frequently cause more destruction than the shiny new ones," said Bob Huber, chief security officer and head of research, Tenable. "Cyberattackers repeatedly find success exploiting these overlooked vulnerabilities to obtain access to sensitive information. Numbers like these conclusively demonstrate that reactive post-event cybersecurity measures aren't effective at mitigating risk. The only way to turn the tide is to shift to preventive security and exposure management." 🔑

ACCORDING TO THE TENABLE REPORT, THE NUMBER ONE GROUP OF MOST-FREQUENTLY EXPLOITED VULNERABILITIES REPRESENTS A LARGE POOL OF KNOWN VULNERABILITIES.

Cyber and ransomware attacks are the enemy of today's data-driven business



Immutability

Preserve data integrity and confidentiality with layers of security and controls



Isolation

Physical and logical separation of data within a vault



Intelligence

Machine learning and analytics help ensure recoverability

DELL PowerProtect
Cyber Recovery



www.cbt.ae



04 2101900



info@cbt.ae

22TB

IN A REIMAGINED HDD

OptiNAND™ TECHNOLOGY



**Ultrastar® DC HC570
22TB* HDD**

**GROW YOUR
DATA, NOT YOUR
FOOTPRINT**

Exponential growth of data means organizations must find ways to efficiently store more data. The Ultrastar® DC HC570 22TB¹ HDD with OptiNAND™ technology is the next leap in high-capacity hard drives, allowing data centers to maximize their storage, especially in footprint- and power-constrained environments.

Learn more at [westerndigital.com](https://www.westerndigital.com).

©2023 Western Digital Corporation or its affiliates. All rights reserved. *1TB = 1 trillion bytes. Actual user capacity may be less depending on operating environment. Western Digital, the Western Digital design, the Western Digital logo, OptiNAND, and WD Purple are registered trademarks or trademarks of Western Digital Corporation or its affiliates in the US and/or other countries. All other marks are the property of their respective owners. Product specifications subject to change without notice. Pictures shown may vary from actual products.

For inquiries, please contact Shuja Kidwai at shuja.kidwai@wdc.com

Available at

ASBIS®

FDC
INTERNATIONAL

 **Redington**
SEAMLESS PARTNERSHIPS