ADVISOR

# The META Experience

**MIDDLE EAST** 

BALLY SINGH, CMO, EVERDOME, TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, ALL ABOUT THE NEW TECHNOLOGICAL BREAKTHROUGH-THE METAVERSE.

# HIGHLIGHTS WOMEN IN TECH



🛞 tahawultech.com





## Manage your network the easy way, through the cloud.



DBS-2000 Series

Nuclias Cloud Managed Switches

Manage your network centrally from any location, without the need to set up a server. Because Nuclias Cloud devices only need plugging in and powering up, it's perfect for businesses that don't have trained IT professionals.

### Who needs Nuclias Cloud



**SMBs & Large Enterprises** 



**Retail Chains** 



Hospitality



Education

# CONTENTS

# Secur







News roundup from the security world in the 6 region and beyond

**2** THE META EXPERIENCE

Jeff Bennison, Director of Security Consulting, 10 Professional Services EMEA, Rackspace Technology, on what ISO/IEC 27002 means to an organisation.

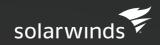


**18** Glen Pendley, Chief Technology Officer, Tenable on how the componue convision Tenable on how the company's acquisition of Bit Discovery will help customers gain better visibility into attack surfaces.



Deepa Kuppuswamy, Information Security Architect, ManageEngine on the changing role of women in the security space.

### 



# Today's IT agility is built on observability.

SolarWinds<sup>®</sup> Hybrid Cloud Observability helps ensure services and online applications are available, operate cost effectively, and deliver a fantastic and predictable digital experience.

- » Modernize IT agility
- » Accelerate cost savings and time to value
- » Resolve issues faster with deep visibility and context
- » Improve user experience and service availability
- » Value across IT Ops, Dev Ops, and security

Learn more about Hybrid Cloud Observability and how we're re-envisioning the solutions you need to drive business results. **Visit solarwinds.com to learn more.** 



# EDITOR'S NOTE



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

> Anita Joseph Editor

**EVENTS** 



## THE META EXPERIENCE

#### Technology is taking us places-literally

and figuratively. While we're progressing by leaps and bounds in areas such as cloud, Al, Machine Learning and more, technology is also fast catapulting us to the 'other world'-the Metaverse, where the virtual is taking us on a physical identity and giving us a unique signature in both worlds. Overwhelmed? Well yes, we've every right to be. As interesting and fascinating as it sounds, the whole Metaverse experience has us worried as well-particularly now that cyber attacks and complex hacking techniques are the norm.

So, how secure is the Metaverse experience? Can we take a leap of faith into the unknown and let technology work its magic? That's what

the cover story in this issue is all about-a safe and secure 'meta' experience. We have Bally Singh, CMO at Everdome discuss this new and exciting frontier of technology and its relentless pace. Singh says that today, there is a need to address emotional, cultural and community safety and security issues as well, since all users have the right security. Our spotlight interview features David Richardson, Vice President, Product Management at Lookout, to find out why

From the Metaverse to data-centric

to enjoy a metaverse that makes them feel

secure

**TECHNOLOGY IS** 

TRANSPORTING US TO

THE OTHER WORLD- THE

**METAVERSE** 

data-centric cloud security is important. Another interview has Glen Pendley, Chief Technology Officer at Tenable, discuss how its acquisition of Bit Discovery will help customers gain better visibility into attack surfaces.

That's not all. We have an exclusive article by Jeff Bennison, Director of Security

Consulting, Professional Services EMEA at Rackspace Technology, on why ISO/IEC 27001 and ISO/IEC 27002 have always been important for organisations to commit to and

be seen as a baseline to identify, measure and improve information security.

We're not revealing more here, the only thing we'd like to point out is that each page in this issue gets more and more interesting with every page turn-it's a mix bag for sure, but one you'll find varied and exciting. HAPPY READING!

Published by

FOUNDER, CPI Dominic De Sousa (1959-2015)

ADVERTISING Group Publishing Director Kausar Syed kausar.syed@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.joseph@cpimediagroup.comm

OnlineEditor

Daniel Shepherd daniel.shepherd@cpimediagroup.com PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan

webmaster@cpimediagroup.com

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

Tel: +971 4 5682993

© Copyright 2022 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.

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com

### ACRONIS SIGNS MINDWARE AS CLOUD DISTRIBUTOR FOR GCC, LEVANT & PAKISTAN TO ADVANCE CYBER PROTECTION FOR REGIONAL ENTERPRISES

#### Acronis has announced its partnership

with Mindware, one of the leading Value-Added Distributors (VADs) in the Middle East and Africa. Mindware will offer the range of Acronis' innovative cloud solutions ranging from cyber security to data protection, to enterprises in Lebanon, Jordan, Iraq, Palestine, Saudi Arabia, Kuwait, Bahrain, Qatar, Oman, UAE, and Pakistan. The partnership will further Mindware's ambitions as a 'Cloud Distributor' with Acronis' strong value proposition in the Cloud protection space.

Acronis offers antivirus, backup, disaster recovery, endpoint protection management solutions, and award-

# Acronis Mindware

winning AI-based anti-malware and blockchain based data authentication technologies through service provider and IT professional deployment models. These solutions protect data, applications, and systems in any environment.

Speaking about the partnership, Silmi Khanfir, Director of Cloud & XaaS said: "We have a clear, strategic objective of being the regional Cloud distributor of choice, by offering our partners aggregated Cloud solutions from various leading vendors and helping them and their customers in their cloud transformation journey. 'Acronis Cyber Protect Cloud' business model perfectly complements our portfolio with a onestop data protection and cybersecurity solution platform."

# COHESITY DELIVERS FORTKNOX - COMBATING RANSOMWARE WITH A SAAS DATA ISOLATION & RECOVERY SOLUTION

#### Cohesity, a leader in next-gen data

management, has announced the general availability of Cohesity FortKnox - a software as a service (SaaS) data isolation and recovery solution, adding to the company's Data Management as a Service portfolio of offerings that run on Amazon Web Services (AWS).

FortKnox is a modern data isolation solution that can play a critical role in helping organisations minimise the impact of cyberattacks such as ransomware. It is designed to provide an additional layer of off-site protection while dramatically simplifying operations and lowering costs compared to magnetic-tape and self-managed data vaults. The SaaS offering also helps enterprises meet recovery service level agreement (SLA) requirements and regulatory requirements.

COICHTY.	(Kar)	
H	Our/deard	27 (A
-	The second secon	ini Million
		 IF - 1 varies   IF - 1 varies

This announcement comes as customers look for a next-gen approach to data management and security. Traditionally, data was air gapped using magnetic tape as part of a 3-2-1 backup strategy - three copies of data, on two different media, with one of them in an off-site environment. Although tape provides security isolation for data it does not allow for rapid recovery at scale, preventing teams from responding quickly to cybersecurity incidents, such as ransomware, where large volumes of data may be compromised.

### LINKSHADOW ACHIEVES INTEGRATION WITH FORTINET THROUGH FABRIC-READY TECHNOLOGY ALLIANCE PROGRAM

#### LinkShadow has announced an

integration combining Fortinet FortiGate Next Generation Firewalls (NGFW) and LinkShadow Cybersecurity Analytics Platform. The integration equips security teams to uncover zero-day threats with proactive threat detection and defence by getting full visibility from Fortinet Firewalls around the defence activities.

Linkshadow Cybersecurity Analytics Platform, the most Innovative User and Entity Behavioral Analytics Platform in Frost Radar for 2020, provides customers with unparalleled detection of the most sophisticated threats. The Linkshadow Cybersecurity Analytics Platform enhances an organisation's defence and accelerates incident response by utilizing Artificial Intelligence based Machine Learning to analyse events, perform UEBA and cutting-edge Threat Hunting.

"Today, most breaches are zero-day exploits, leaving no scope for detection or mitigation. Lack of timely intelligence cripples security teams, posing a panic situation, and brings businesses to a stand-still followed by huge financial ramifications," said Fadi Sharaf, Regional Sales Director, LinkShadow. "It is critical to deploy automated cybersecurity tools driven by Artificial Intelligence that can detect and mitigate an anomaly well in



advance and save the day. With this robust integration, LinkShadow gains full visibility into the application layers to monitor abnormal connections and data exfiltration which are proactively stopped by FortiGate Next Generation Firewall before posing a threat," Fadi Sharaf added.

#### **ESET LEADER IN G2 SUMMER REPORT FOR ESET PROTECT ADVANCED**

#### ESET, a global leader in digital security,

has been awarded Leader status in G2's report for summer 2022. The ESET PROTECT Advanced solution has consistently been highly ranked by G2 users and achieved substantial satisfaction and market presence scores in their Grid Reports, which represent the democratic voice of real software users, offering benchmarks for product comparison and market trend analysis. In the summer edition of the G2 Grid Reports, ESET was a Leader in several of the reports, including for Antivirus Software, Endpoint Management Software, Endpoint Protection Suites, and Mobile Data Security Software.

In terms of the Mid-Market reports aimed at companies with up to 1,000 employees, ESET was a Leader in Mid-Market Endpoint Protection Suites, Mid-Market Antivirus Software, and Mid-Market Endpoint Management Software.



### SOLARWINDS UNVEILS NEW SOFTWARE DEVELOPMENT PROCESS

SUDHAKAR RAMAKRISHNA

### **SolarWinds, a** leading provider

of simple, powerful,

and secure IT management software, has unveiled its new Next-Generation Build System, a transformational model for software development. The new software build process is a key component of the company's Secure by Design initiative to make SolarWinds a model for enterprise software security.

The software development and build process improvements were made in an accelerated timeline over the past year in response to the highly sophisticated SUNBURST cyberattack, which targeted SolarWinds and other technology companies. The Next-Generation Build System includes both new software development practices and technology to strengthen the integrity of the build environment. This consists of the firstof-its-kind "parallel build" process, where the development of SolarWinds software takes place through multiple highly secure duplicate paths to establish a basis for integrity checks.

"Communicating transparently and collaborating within the industry is the only way to effectively protect our shared cyber infrastructure from evolving threats," said Sudhakar Ramakrishna, president and CEO, SolarWinds. "Our Secure by Design initiative is intended to set a new standard in software supply chain security via innovations in build systems and build processes. We believe our customers, peers, and the broader industry can also benefit from our practices."

### COMMVAULT & ORACLE PARTNER TO DELIVER METALLIC DATA MANAGEMENT AS A SERVICE ON ORACLE CLOUD INFRASTRUCTURE

#### Commvault, a global enterprise leader

in intelligent data services across onpremises, cloud, and SaaS environments, has expanded its strategic partnership with Oracle to include Metallic DMaaS on Oracle Cloud. As part of Commvault's multi-cloud strategy, Metallic's industryleading services will be offered on Oracle Cloud Infrastructure (OCI) and available in all commercial OCI regions globally.

"Resilience has never been more critical than it is today," said Sanjay Mirchandani, president and Chief Executive Officer, Commvault. "Our partnership gives customers the trusted industry-leading solutions they need to rein in data sprawl and protect their data in an unrelenting E ON CTURE threat landscape. All

while accelerating their critical cloud journeys."

In the fight against ransomware and cyberattacks, Metallic DMaaS helps protect data from corruption, unauthorised access, and other threats across vital sectors of business, including insurance, financial services, manufacturing, and defence. With Metallic DMaaS, customers can easily back up their digital footprint in any consumption model, from cloud-native to on-premises workloads, including databases, virtual machines, Kubernetes, and file and object storage.

### MANAGEENGINE CITED AS A STRONG PERFORMER FOR UNIFIED ENDPOINT MANAGEMENT TOOLS

#### ManageEngine, the enterprise IT

management division of Zoho Corporation, has announced that it has been acknowledged as a Strong Performer in The Forrester Wave(TM): Unified Endpoint Management (UEM), Q4 2021.

The recognition is based on the evaluation of ManageEngine's flagship UEM software, Desktop Central. The evaluation is based on 24 different criteria focused around current offerings, strategy and market presence.

"The endpoint management space has evolved from client management to enterprise mobility management, to UEM and now to endpoint security integrated with UEM. Over the years, we have developed all these capabilities in-house to meet market requirements at every stage. This organic approach allows us to MATHIVANAN VENKATACHALAM

provide a unified agent for all necessary workflows and added capabilities at no additional integrations or setup," said Mathivanan Venkatachalam, Vice President of ManageEngine, in response to the recognition.

ManageEngine was recognised in the report for its cost-effectiveness and diverse customer base in terms of geography, industry and size. Its unique OS deployer was cited for enabling fast imaging irrespective of the hardware. The company received the maximum possible score in the criteria of traditional client management, patching and remote support, in addition to performance and planned enhancements.

### **KASPERSKY DISCOVERS NEW BACKDOOR TARGETING GOVERNMENTS** & NGO ORGANISATIONS ACROSS META

#### Kaspersky experts have brought to light a

poorly detected SessionManager backdoor that was set up as a malicious module within the Internet Information Services (IIS), a popular web server edited by Microsoft. Once propagated, SessionManager enables a wide range of malicious activities, starting from collecting emails to complete control over the victim's infrastructure.

First leveraged in late March 2021, the newly discovered backdoor has hit governmental institutions and NGOs across the globe with victims in eight countries from the Middle East, Turkey and Africa region, including Kuwait, Saudi Arabia, Nigeria, Kenya and Turkey.

Dubbed SessionManager. the backdoor enables threat actors to keep persistent, update-resistant and rather stealth access to the IT infrastructure of a targeted organisation. Once dropped into the victim's system, cybercriminals behind the backdoor can gain access to company emails, update further malicious access by installing other types of malware or clandestinely manage compromised servers, which can be leveraged as malicious infrastructure.



### VECTRA BECOMES AWS SECURITY COMPETENCY PARTNER

#### Vectra AI, a leader in threat detection

and response, has announced that it has become an Amazon Web Services (AWS) Security Competency Partner further confirming its technical expertise and proven customer success when further safeguarding AWS environments. The competency designation recognises that Vectra has demonstrated deep cloud security expertise and has proven technology that helps customers further enhance their security measures across hybrid architectures and cloud environments.

An AWS Security Competency differentiates Vectra as an AWS

Partner Network (APN) member that provides specialised threat detection technology designed to help enterprises adopt, develop, and deploy complex security projects on AWS. To receive this designation, APN members must possess deep AWS expertise and deliver solutions seamlessly on AWS. Vectra achieved its AWS Security Competency status through a rigorous qualification process based on references and feedback from its customers.

"Becoming an AWS Security Competency Partner is an exciting milestone for Vectra and for many of our customers who leverage AWS as



a critical component in their everyday operations," said Michael Porat, Vectra SVP, Corporate and Business Development. "Solving threat detection and response challenges for our customers is top priority and this competency further validates our ability to do that in the cloud and wherever organisations choose to configure their environments."

# ISO/IEC 27002 UPDATE: WHAT DOES THAT MEAN?

**JEFF BENNISON**, DIRECTOR OF SECURITY CONSULTING, PROFESSIONAL SERVICES EMEA, RACKSPACE TECHNOLOGY



dherence to strong cyber security standards is as important as ever for companies in, and trying to sell to, highly regulated industries, such as financial services, government, and critical infrastructure. Not only does it ensure they understand their organisational risk and keep their data safe, but it could make the difference when securing contracts with companies that demand cyber excellence across their supply chain. As such, organisations must ensure

As such, organisations must ensure they are keeping up to date with the latest standards and they don't leave themselves exposed. Earlier this year, the ISO/IEC 27002 information security standard underwent a series of highly welcome updates that security teams now need to implement to remain compliant. The standard is the associated document to ISO 27001, last revised in 2013, and gives detailed implementation guidance for these existing directives. Many of the new controls outlined in the update ensure businesses are adapting to the new security landscape. For example, with the explosion of cloud in recent years, there was an impending need to implement controls around 'Information security for the use of cloud services (5.2.3)'. 'Data leakage prevention (8.12)' and 'Data masking (8.11)' are also in direct response to recent breaches.

ISO/IEC 27001 and ISO/IEC 27002 have always been important for organisations to commit to and should be seen as a baseline to identify, measure and improve information security. However, what do these changes mean to businesses and how can they comply with the updated standard?

### How does the update impact my organisation?

Let's start by looking at the changes. Key revisions in the latest standard include:

- The phrase "Code of Practice" has been omitted from the title of the ISO/IEC 27002. This is to enable readers/implementors to understand its purpose as an ISO/IEC 27001 reference for control description and application.
- The number of controls has also been streamlined from 114 down to 93, with the remaining clauses now grouped into four clear sections – Organisational, People, Physical and Technological. Similarly, a total of 23 controls have been renamed to enable an easier understanding and implementing of them.
- 11 new controls have been added to reflect the changing security landscape. These include Threat intelligence, Information security for the use of cloud services, Data

#### ISO/IEC 27001 AND ISO/IEC 27002 HAVE ALWAYS BEEN IMPORTANT FOR ORGANISATIONS TO COMMIT TO AND SHOULD BE SEEN AS A BASELINE TO IDENTIFY, MEASURE AND IMPROVE INFORMATION SECURITY.

masking and Secure coding. These changes address both the controls themselves and how to use and organise them. The Information Security Management System (ISMS) risk management process allows organisations to select controls to reduce organisational risk at will, from anywhere. Obviously, the focus relies on the controls contained within ISO/ IEC 27002. If an organisation selects controls from sources other than ISO/ IEC 27002, they must be compared to ISO/IEC 27002 and any variance justified and documented.

Any organisation currently certified to ISO/IEC 27001:2013 can continue referencing and selecting the controls within the current ISO/IEC 27002:2013. Alternatively, they have an option to utilise controls in the new version (as part of the Information Security Review process) if they wish. Like any update to a standard there is a transition period. In this case that period is two years, which starts from the date of the release of the updated ISO/IEC 27001 – so there is plenty of time to plan.

### Managing the update as a certified organisation

During the transition, certified organisations will need to perform a risk treatment review to ensure it is aligned with the document structure and new control numbering. They will also need to edit their Statement of Applicability ensuring new controls are accurately listed, and review and edit/update accordingly the ISMS documentation to reflect the changes. There may also be some documents which do not exist and need creating and implementing.

ISO/IEC 27001 is already document heavy, so this is the area which is likely to require the most effort. The new ISO/ IEC 27002 includes an annex identifying the 2013 standard to ease the process of implementing the new version.

#### Ensuring a successful transition

Whether an organisation chooses to certify due to an internal desire to understand the risks it is facing or external pressure from due diligence/ right to audit activity, managing this transition correctly is essential. With ISO/IEC 27002, you can become uncompliant very quickly, but by engaging a third party to perform tasks like scope reviews, gap analysis, user awareness training or simply creating documentation, you can make this process far more seamless.

Effective implementation of these standards will help organisations to identify suitable and proportionate security controls within the process of setting up an ISMS, and enable them to achieve best practice in information security management. It will also help them to meet any legal, statutory, regulatory, and contractual requirements in relation to information security. But ultimately, it will enable them to strengthen their risk management and reduce the likelihood of information security breaches.

# THE META EXPERIENCE

# **BALLY SINGH,** CMO, EVERDOME, TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, ALL ABOUT THE NEW TECHNOLOGICAL BREAKTHROUGH-THE METAVERSE.

ell us all about Everdome's hyper-realistic Metaverse 3.0 experience.

#### As the metaverse disrupts the existing technological landscape, how secure would you say is the whole experience?

The metaverse is a new territory - a new technological frontier. As with any other frontier, it requires us to develop new tools and practices to tackle previously unheard of challenges. We need to consider and develop a range of new safety and security measures that cover a variety of aspects across the metaverse ecosystem - such as solutions to protect assets, devices, intellectual property,

users' identity and personal details. There's even a need to address emotional, cultural and community safety and security, as all users have the right to enjoy a metaverse that makes them feel secure.

And yet despite the need and expectation for high levels of security, as users we don't want those measures to be constantly in our face. They need to feel ambient and seamlessly integrated into either the background or common processes. We want convenient security that is reliable, allencompassing, and requires as little effort as possible with the reassurance that every aspect of metaverse safety has been taken into consideration.

One of the greatest advantages we have



is that we're able to build these features in from the ground up, rather than having to retrofit them. This gives us the opportunity to adopt a highly conscious design and compliance process, which is the best possible approach we can implement in Everdome at this stage. Naturally though security is an everevolving issue. We will continue to use cutting edge technology based on the latest frameworks and best practices to provide an environment that is as seamlessly secure as possible.

Our DevOps team constantly updates all necessary components based on daily updates, and our end users will receive updates on a weekly basis. In addition to this, our Compliance team is focused on constantly improving content and experience quality. This helps us to ensure that emotional and cultural safety is a priority, by ensuring that people cannot promote, show or share content that goes against our general rules.

#### Is there a public reluctance to completely embrace all of the Metaverse excitement, owing to security concerns?

No, I don't believe so. As humans we are naturally cautious of anything new, and that includes innovations in technology

THE MARKETING AND HYPE AROUND THE METAVERSE HAS DEFINITELY OUTPACED THE ADOPTION OF THE TECHNOLOGY, BUT THAT TENDS TO BE THE CASE WHEN IT COMES TO NEW TECH.



and software offerings. You only need to look back into relatively recent history when the internet had its beginnings to see how rapidly we change our minds and embrace new technology - at first, the internet was widely criticised and came under considerable doubt, but now it's an integral part of our lives.

Building a wider understanding of exactly what the metaverse is and what it can offer is going to drive acceptance, at least in its most basic form. There is the possibility for it to be quite a steep learning curve, because the metaverse brings together numerous new technologies - such as blockchain and cryptocurrency, for example. With that said though, these two technologies in

### A SUCCESSFUL METAVERSE WILL BE ABLE TO DELIVER ON ITS PROMISE FOR MEANING AND PURPOSE, WITH THE ABILITY TO ADDRESS THE NEEDS OF ITS AUDIENCE, PROVIDE TECHNOLOGICAL STABILITY AND SECURITY.

particular are increasingly adopted and accepted in the world around us, which will contribute to people having a better understanding of at least two aspects of the metaverse.



The marketing and hype around the metaverse has definitely outpaced the adoption of the technology, but that tends to be the case when it comes to new tech. Any research you find online right now about the metaverse is anecdotal, based on individuals' visions for the future.

Beyond creating more understanding, there is also the need to consider that users need to see and embrace both meaning and purpose in the metaverse. For some metaverses, the purpose will be purely another form of entertainment. Others will be all about community, interaction, communication or trading. A successful metaverse will be able to deliver on its promise for meaning and purpose, with the ability to address the needs of its audience, provide technological stability and security. This will help to iron out any remaining barriers for adoption.

#### How does Everdome, in particular, address this issue and ensure the security of the metaverse experience?

To elaborate on what I've mentioned already, we have a DevOps team that constantly seeks new ways in which to enhance security and safety throughout our metaverse ecosystem, from a technology and software perspective in particular. Additionally, we have a dedicated Compliance team that will work to ensure a safer community experience, so that any content that may go against our rules is handled swiftly and seamlessly. We will regularly monitor the Everdome environment

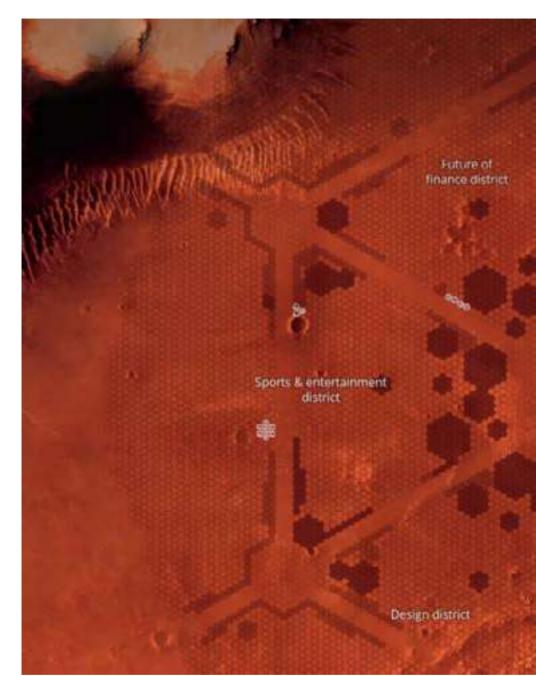
#### COVER STORY / EVERDOME

both manually and automatically via algorithms. There will also be a public reporting tool, which will allow all users to flag content they feel is inappropriate and it will also show them things that are blocked, along with reasons for blocking. Beyond this, we will offer community consultations to ensure that the peoplecentric element of our metaverse runs as smoothly as possible for all users.

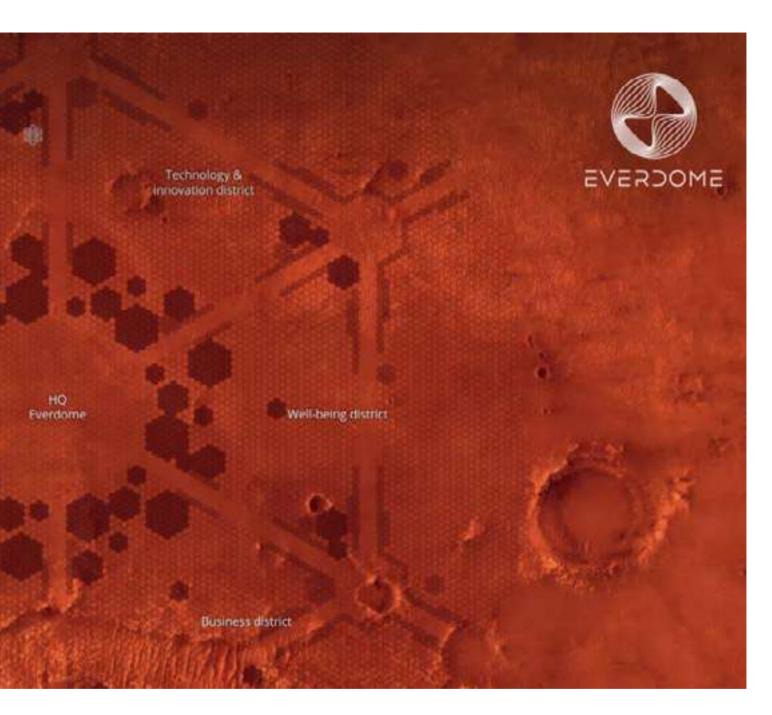
What are some of the challenges, particularly with regard to security frameworks and technology scaling, that Everdome & the metaverse experience faces in its journey of growth and evolution?

As the metaverse is still a new concept. there are a number of challenges that we need to overcome - which may sound slightly ominous but the reality is that every new technology will go through the same processes. Everdome has a strong, talented team that makes challenges easier to overcome; we're very confident in the team's ability and drive to deliver excellence. In fact, talent can be a challenge in itself. We've hired some brilliant people to build secure and scalable solutions. Based on previous experiences, we knew it was crucial to have the right people in the right positions with the right technology, from the very beginning.

In terms of actual challenges, interoperability of design and security frameworks throughout the metaverse ecosystem is one example of an issue that needs to be addressed and overcome.



WE'VE BUILT A SOLID TEAM OF EXPERTS TO TAKE CARE OF EVERY ASPECT OF EVERDOME, FROM BACK-END CODE AND TECH TO GRAPHICS, MARKETING AND MORE, SO THAT OUR USERS CAN ENJOY THE BEST POSSIBLE EXPERIENCE WITHIN OUR METAVERSE. On the non-tech side of things, brand reputation and user trust must be built. We're considering both of these aspects in the very heart of Everdome's design and governance processes. After all, at the end of the day Everdome is an environment for people to enjoy, so it makes sense to consider our users' needs and wants every step of the way. This also means being rock solid in our intentions, value system and design



decisions, backing them up with actual product experiences.

There are also matters such as cost optimisation. Everdome has already garnered a lot of international attention in the lead-up to its launch later this year, so we need to be prepared to handle huge traffic... which can be costly. To be as cost-effective as possible we use Amazon Web Services. This allows us to simply upor downscale our servers as needed, allowing us to be agile in handling traffic while saving money.

We also have the matter of smart contracts. These are based in blockchain, and are therefore relatively new. They have to be well written and well audited, because once you deploy a smart contract there's no way back. We've invested in hiring top developers and leading agencies to audit the code, ensuring things in that department run as smoothly as possible.

So yes, there are challenges - quite a few of them - but nothing that can't be overcome. We've built a solid team of experts to take care of every aspect of Everdome, from back-end code and tech to graphics, marketing and more, so that our users can enjoy the best possible experience within our metaverse. **1** 

# ALL ABOUT VISIBILITY

**GLEN PENDLEY,** CTO, TENABLE, ON HOW ITS ACQUISITION OF BIT DISCOVERY WILL HELP CUSTOMERS GAIN BETTER VISIBILITY INTO ATTACK SURFACES.

ell us more about Bit Discovery.

Bit Discovery employs a multi-phased approach of identifying what assets and services a particular brand(s) has residing on the Internet.

It has built one of the largest attack surface maps in the world using 500 data sources to identify more than 5 billion assets. The technology combines IP addresses, hostnames, ports, website URLs, WHOIS records, Autonomous System Numbers (ASN) data, and much more, to discover assets and help security teams establish their complete digital footprint in just a few minutes. And automation allows security teams to not only enumerate known assets, but continuously discover unknown assets every 24 hours.

However, Bit Discovery goes beyond

providing automated external asset discovery. It also provides extensive context and attribution details for each asset with over 150 metadata fields such as CMS type, TLS certificate status, geo-IP physical location, and cloud or CDN provider. This additional context is critical for helping cybersecurity teams determine asset criticality, identify asset ownership and help make more informed decisions based on potential exposure.



#### How is the Tenable-Bit Discovery acquisition expected to benefit the regional market/customers?

Visibility remains at the heart of cybersecurity today — of assets, data, exposures, privileges, threats — full and complete discovery is essential in order to adequately defend against adversaries and cyber criminals.

On completion of this acquisition, we announced our plans to leverage

Bit Discovery's EASM solutions across our entire portfolio – from enterprise VM to Nessus, from cloud to OT to identity – boosting security effectiveness dramatically. Once integrated, customers will have the ability to assess the security posture of their entire attack surface with one solution and understand each of these in the context of an attack path which might exist from external systems to critical assets or any other part of the enterprise.

For our customers in the Middle East, they will be able to address one of cybersecurity's most elusive goals — a differentiated 360-degree view of the modern attack surface, both inside out and outside in, on-premises and in the cloud, to identify and eliminate areas of known and unknown security risk.

#### Why is attack surface management becoming increasingly relevant to modern cybersecurity?

There is a saving that to catch a thief you need to think like a thief and the same is true in cybersecurity. The best way to determine what risks exist within the infrastructure is to consider what attack paths exist and how a threat actor might exploit them. One example is that, whatever is visible on the internet, is likely to be the first point threat actors will target. To avoid new points of security vulnerability and to ensure good organisational risk management, it is critical for organisations to have visibility into and to understand both known and previously unknown internet-facing assets and address these entry points.

#### Do you think lack of visibility into attack surfaces is the main challenge facing organisations in the region today?

In short, yes. Gaining comprehensive visibility and discovering all assets across the attack surface is challenging. Many assets are highly dynamic and ephemeral in the era of cloud, which means they can be difficult to detect VISIBILITY REMAINS AT THE HEART OF CYBERSECURITY TODAY, AND FULL AND COMPLETE DISCOVERY → IS ESSENTIAL IN ORDER TO ADEQUATELY DEFEND AGAINST ADVERSARIES.

using traditional scanning. New asset deployments are becoming decentralised with many application and development teams across different business units and subsidiaries spinning up their own cloud workloads and web applications without informing their cybersecurity teams. Mergers and acquisitions create even more challenges as the parent organisation often has limited visibility into the acquired company's external attack surface. And there is tremendous asset sprawl with many assets outliving their initial use and running without ongoing upkeep or lifecycle management. The result is that many organisations can only see a fraction of their digital footprint, leading to significant blind spots and pockets of cyber risk.

#### What are some of the leading cybersecurity trends in the region today?

What we see coming out of the region is not unlike what we see everywhere else in the world. The overwhelming majority of cyber attacks happen because people do not have the visibility needed to apply the proper cyber hygiene to the systems and users that are at most risk. Sadly, this is not a new trend and it applies as much to the organisations in the Middle East as it does everywhere else in the world.

# Celebrating Clomen POWER IN TECHNOLOGY

Active and a second and a sec

The very first edition of the Women In Technology Forum & Awards was held in June, celebrating women power and honouring the remarkable ladies who innovate, inspire and transform the technology sector as we know it.

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, will be the focus of the Women in Tech (Pride of Tech) conference and awards.

While the awards aim 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 will highlight the exceptional efforts made by women to break digital boundaries and create a more inclusive global workforce. This year, the focus is on growth, continuity and results driven by women– particularly how they've emerged stronger despite the socio-economic challenges over the past two years.



Diana El Kara Infor



Selina Bieber GoDaddy

Konica Khandelwal

www.tahawultech.com



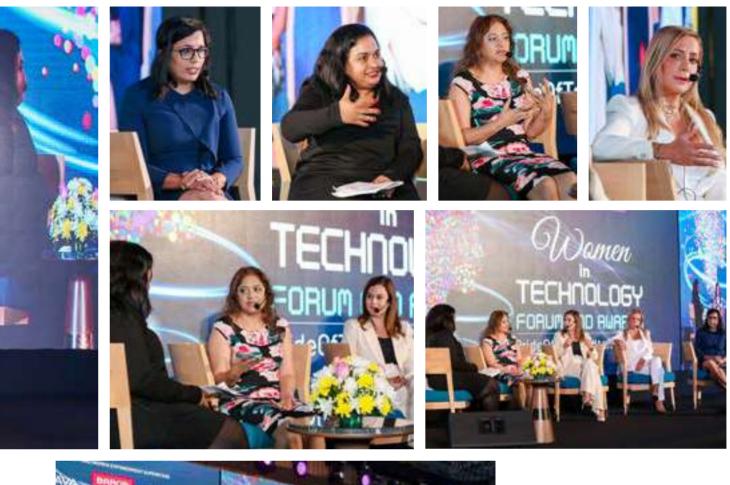




# BREAKING BOUNDARIES

ANITA JOSEPH, EDITOR, RESELLER ME, SECURITY ME & TAHAWULTECH.COM, MODERATED A PANEL DISCUSSION AT THE WOMEN IN TECH FORUM & AWARDS HELD RECENTLY.

he discussion, titled **Driving Change With Purpose & Impact**, featured four frontrunners of the technology space: **Maya Zakhour**, Director-Partner Sales Organization Area Lead- Eastern Europe, Middle East, Africa, Turkey (META), Iberia, & Latin America, **Kinda Baydoun**, Regional Manager -Channel & Distribution at VEEAM Software Middle East, **Mansi Shah-Gandhi**, Regional Technology Lead, MEA, Rackspace Technology & **Joumana Karam**, Head of Marketing & Product Business Unit, ACER.





While the panelists all agreed that while being a woman in the technology space was exciting, it was by no means easy. Still, they agreed that it was a dream in their hearts, passion for a cause and determination to stick it out no matter the odds, was what kept them going in a career space that is intensely competitive and dynamic. The discussion focused on how women have been driving change with their natural, inborn qualities of empathy, vision, detailed planning and balanced decision making. It also highlighted the need for exceptional mentors at an early career stage, the willingness to experiment and the need to think out of the box. THE PANEL UNDERSCORED THE EXCEPTIONAL EFFORTS MADE BY WOMEN TO BREAK DIGITAL BOUNDARIES AND CREATE A MORE INCLUSIVE GLOBAL WORKFORCE.

In short, the panel underscored the exceptional efforts made by women to break digital boundaries and create a more inclusive global workforce. The spotlight 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.



# **DATA-CENTRIC SECURITY**

ANITA JOSEPH CAUGHT UP WITH **DAVID RICHARDSON**, VP, PRODUCT MANAGEMENT, LOOKOUT, TO FIND OUT WHY DATA-CENTRIC CLOUD SECURITY IS IMPORTANT.

#### ow critical is data-centric cloud security today for organisations?

**David:** So, any organisation that is doing digital

transformation, moving data into the cloud, they need to be thinking about where their data is going, how they control that data and whether their existing security controls will enable them to understand where their data lives, and who its being shared with. And so its absolutely critical for any organisation that is moving data from on-prem to the cloud. When you think of moving data from on-prem to the cloud, even a project like moving to Office 365, that would qualify here, because you have all this core intellectual property that exists – excel spreadsheets and word documents.. SharePoint that you had on-prem that you had full control of, which is now moved completely into the Cloud or moved into OneDrive. If you look at the way people used to control and protect their data, it used to be, as I'd like to call it, hard drive centric, where you might have put some controls in place, to avoid someone from downloading a file, copying it to a USB stick and handing it to someone else. But that's not the way organisations are sharing data anymore. Once you've adopted the Cloud, these things are

Cloud-accessible. And when you share data from one user to another, whether its internal or external, you are using Share button that is in the upper right-hand corner of the web app that you are using and you are typing in someone's email address. Nothing is getting downloaded to your hard drive. Nothing is getting attached to an email and then sent to someone else's machine so that they can be downloaded there. So the policies and controls that organisations are putting in place, often they are very hard drive or network centric. So they need to see the data being downloaded or they need to see the data getting written onto the hard drive in order for you to be able to protect that. These days that's just not how data is being shared as organisations adopt Cloud technologies. So you just have a bunch of policies - I would call them paper policies - that are not being enforced, just based on the way technology has changed underneath them.

#### Are organisations doing enough to ensure data centric cloud security and what is lacking?

David: I would say that the main steps that organisations are taking is that they are trying to understand and measure cloud services that are being used. especially unauthorised cloud services like shadow IT – what services are being accessed by my employees, how are they using these things to share data. You see this from everything – for example – the adoption of Dropbox, because it's a more convenient experience to share data with your co-workers or partners. Or you see it on a small scale too – a popular app has been spreading through enterprises recently called 'Calendly' - it's like a really easy way to book an appointment with someone, share what open slots they have in their calendar etc. This is I would say a grass-roots kind of an adoption of a cloud service like that, where somebody used it to book an appointment once, they had a good experience, and they started using it to book appointments with their clients...

#### ORGANISATIONS NEED TO SEE THE DATA BEING DOWNLOADED TO BE ABLE TO PROTECT THAT.

and before you know it, a third of the organisation's calendar data is being shared with some third party that they are not really familiar with. So, when it comes to shadow IT, organisations are doing a little bit there, but most organisations are not really going beyond that – which is even understanding – "hev even for my sanctioned cloud adoption. I need to be able to put security controls in place and understand what data lives where, who is it shared with, how do I ensure that only appropriate data is shared with appropriate individuals... that I don't have compliance problems like healthcare data leaking out of the organisation, or customer records leaking out of the organisation." Most organisations are not at that point yet. They are really at the point of understanding what cloud services are being adopted.

#### Tell us about Lookout, its presence in the region and how it is helping regional organisations with their Digital Transformation goals?

David: We are a global business, safeguarding data for thousands of businesses around the world, including some extremely large enterprises, government customers, small businesses, as well as tens of thousands of individuals. Our presence in the Middle East is growing fast. We've got customers in UAE. Saudi Arabia. Jordan. Kuwait. Qatar., across all sorts of verticals - financial services, government, transportation, manufacturing, energy etc. Kuwait Integrated Petroleum Industries Company (KIPIC) for example, we've done a case study on how they are protecting their workforce using

Lookout's endpoint and cloud security capabilities. So, I would say we have a wide range of customers throughout the region. It's really about adoption of SaaS services and moving data to the cloud. That's the main driver for this kind of business. I think another thing that is unique to the region is there's a lot more concern about Advanced Persistent Threats (APTs) such as Pegasus developed by the NSO Group, that is very targeted attacks on senior executives in order to compromise their devices and understand all data that is flowing to and from those devices. So there is extra concern around corporate or state espionage that creates more specialized use cases in the region.

#### What can the C-Suite do to ensure robust security strategies for organisations so that they can fast track their digital transformation goals without compromising their data?

**David:** So, there is always a balance right? You want to enable your employees to work productively. That's the goal at the end of the day. You can lock everything down and no one can get anything done. And you might be secure, but you are also going to go out of business. I would say that you should embrace the cloud, you should embrace modern productivity tools and capabilities and you should work towards enabling your employees to be productive. That being said, you need to adopt modern security tools in that process, such as a Secure Access Service Edge (SASE) solution that allows you to see all the data that's flowing to and from your cloud services. Especially you should select a solution that gives you full control like you had before over all the data flowing to and from those services – like those hardware centric controls you had in the past, you need to find systems and tools – a good SASE product will do that for you. It will enable you to regain that control so that you know where that data lives, who has access to it and you can revoke that access at any point of time. 1

# SEAGATE REVOLUTIONISES DATA PROTECTION & STORAGE WITH THE INTRODUCTION OF EXOS 2U12 SOLUTION

THE EXOS 2U12 STORAGE SOLUTION IS IDEAL FOR THOSE CUSTOMERS WHO SEEK A BALANCE OF PRICE, PERFORMANCE, AND STORAGE DENSITY.

he Exos 2U12 Storage Solution that recently entered the market is taking on the storage solutions industry by storm. Entering at a competitive price point, the Seagate Exos X 2U12 delivers advanced data protection, capacity and performance. The technologically-advanced storage solution is currently being implemented by a luxury hotel in Downtown Dubai – the central hub for safe and secure tourism. The space-saving storage block is efficient, agile, and scalable and can support cables, universal ports, configuration controls and standard zoning.

#### Optimises Capacity and Delivers Consistent High Performance

The Exos 2U12 Storage Solutions that has a maximum throughput of 14.4 GB/s in a single I/O module or 28.8GB/s in a dual controller configuration, works on leveraging both speed and performance and is designed to assist even the

ENTERPRISE



smallest of businesses to get data to their respective applications at the speed of light.

The impressive Exos Solution is 95% faster than comparable solutions that are reliant on low-cost, low-capacity hard disk drives (HDD) and are often used to minimise storage expenses and so you THE SPACE-SAVING STORAGE BLOCK IS EFFICIENT, AGILE, AND SCALABLE AND CAN SUPPORT CABLES, UNIVERSAL PORTS, CONFIGURATION CONTROLS AND STANDARD ZONING.



can rest easy knowing that the system will operate at maximum capacity while offering optimum security.

#### Delivers Versatile Infrastructure That Can Be Built to Scale

The Exos 2U12 Storage Solution is designed for administrators that require a compact storage solution that can pair and integrate to the scale of the business and is the ideal solution for those customers who seek a balance of price, performance, and storage density.

The storage solution can expand up to 144 SSDs and hard drives. By using this flexible solution that is easy to set up, maintain and expand with the use of interchangeable FRUs and hotswappable components, users now have the ability to gain instant virtual access to their stored data and can save space with up to 12 drives in a 2U rackmount enclosure.

#### **Easy Access to Critical Data**

The Exos 2U12 Storage Solution marries cost efficiency with high volumes of data availability. Providing up to 99.999% of data, the solution's architecture, data replication and fast streaming allow for access to data to be uninterrupted and fool-proof. The solution also comes equipped with the exclusive Seagate ADAPT data protection technology that enables and supports fast and efficient drive rebuilds that intend to completely eliminate system downtime.

#### Go Green with Exos 2U12

The solution that meets the stringent global requirements for recycling, is not only environmentally conscious but also houses an agile system that adapts as the use cases evolve and the need for capacity increases. The datasphere is well-matched for the small-tomedium business market thanks to its competent management capabilities and high capacity that helps minimize environmental impact.

#### Places Security as Its Main Priority

When looking at storage solutions, it is no secret that companies and users value security above all else. The Exos 2U12 Storage Solution comes equipped with Seagate Secure cybersecurity features and intelligent firmware that not only provides easy access to stored data, but also allows for reliable and safe file access, transfer and management.

The Seagate Exos 2U12 is the perfect addition to any small-to-medium business that is on the lookout for a fast, easy and reliable storage solution. The technology produced by Seagate in a cost-efficient way is like no other and is set to be considered to be a serious competitor against other such storage solutions in the market.

### THE STORAGE SOLUTION COMES EQUIPPED WITH SEAGATE SECURE CYBERSECURITY FEATURES AND INTELLIGENT FIRMWARE THAT PROVIDES EASY ACCESS TO STORED DATA AND ALLOWS FOR RELIABLE & SAFE FILE ACCESS, TRANSFER AND MANAGEMENT.



Co-organiser

Host Organisation



غرفية الوظيب ABU DHABI CHAMBER



**Destination Partner** 

UI 5 0 المؤتمرات والمعارض CONVENTION & EXHIBITION BUREAU

### **12 - 14 SEPTEMBER 2022**

Hall Nos 3 & 4, Abu Dhabi National Exhibition Centre (ADNEC), UAE Show Timings: 10:00 AM - 4:00 PM

## The only event in Middle East dedicated to the manufacturing and industrialisation industry

Co-located show



#### WHY VISIT



Connect with peers from all across the



Witness live demos & new product launches under niche segments



Discover the latest technologies focused on the manufacturing and industrialisation industry



Gain knowledge & insights by attending an interactive workshop on Manufacturing & Tech Talks



Network with policymakers, government bodies, existing distributors and obtain insights into existing and future projects



**SUPPORTERS** 



www.memanufacturingandtechnology.com

# 1 IN 5 HTML EMAIL ATTACHMENTS MALICIOUS: STUDY

NEW RESEARCH CONDUCTED BY BARRACUDA NETWORKS, A LEADING PROVIDER OF CLOUD-FIRST SECURITY SOLUTIONS, HAS FOUND THAT HTML ATTACHMENTS ARE BY FAR THE MOST USED BY CYBERCRIMINALS FOR MALICIOUS PURPOSES.

ATTACKERS DO NOT INCLUDE MALWARE IN THE ATTACHMENT ITSELF BUT INSTEAD USE MULTIPLE REDIRECTS WITH JAVA SCRIPT LIBRARIES HOSTED ELSEWHERE. by Barracuda Networks, Inc., a leading provider of cloud-first security solutions, has found that HTML attachments are by far the most used by cybercriminals for malicious purposes. The company's analysis of millions of email attachments over the past month revealed that a whole 1 in 5 HTML attachments were malicious. By comparison, a meagre 0.03% and 0.009% of MS Office and PDF files respectively that were sent via the scanned emails were found to be malicious.

ew research conducted

Explaining the growing popularity of HTML attachments as an attack vector, Toni El Inati - RVP Sales. META & CEE. Barracuda Networks said, "HTML attachments have become ubiguitous in email communications as they're commonly used for system generated reports, updates, and notifications. They often include hyperlinks which users have become accustomed to clicking without first checking to see the full URL. It's no surprise then that attackers have been guick to exploit this trust. Moreover, these attachments mean that attackers no longer need to place malicious links in body of the email and therefore allow them to bypass traditional anti-spam and anti-virus policies with ease."

In analysing the modus operandi of



the cybercriminals perpetrating these attacks, Barracuda's experts found credential phishing and malware to be primarily motives. The research revealed that attackers commonly embed links to phishing or malicious websites within their HTML attachments. When opened, these HTML files use Java script to redirect users to third-party machines and request that they enter their credentials to access information, or download a file that may contain malware.

Barracuda's researchers pointed out that these attacks are difficult to detect because the HTML attachments themselves are not malicious. Attackers do not include malware in the attachment itself but instead use multiple redirects with Java script libraries hosted elsewhere. Potential protection against these attacks must therefore consider the entire email along with its HTML attachments, looking at all redirects and analysing the content of the email for malicious intent.

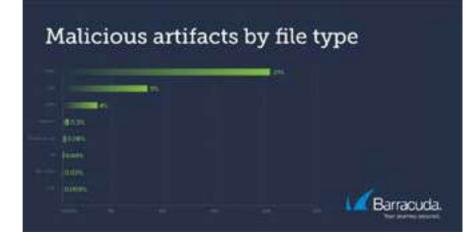


The company's cybersecurity experts also outlined key ways in which organisations can protect against the growing threat of malicious HTML attachments:

• Ensure the organisation's email protection scans and blocks malicious HTML attachments. These can be hard to identify accurately,

and detection tool often include a large number of false positives. The best solutions will include machine learning and static code analysis that evaluate the content of an email and not just an attachment.

• Train users to identify and report potentially malicious HTML attachments. Given the volume of



these type of attacks, users should be wary of all HTML attachments, especially those coming from sources they haven't seen before. Organisations should include examples of these attacks as part of their phishing simulation campaigns and train users to always double check before sharing their login credentials.

 If malicious emails get through, have post delivery remediation tools ready. These must allow the organisation to quickly identify and remove any instances of malicious email from all user inboxes. Automated incident response can help do this quickly before attacks spread through an organisation, and account takeover protection can monitor and alert security teams of suspicious account activity if login credentials were to be compromised. 1

# **HUMAN RISK IS BIGGEST THREAT TO CYBERSECURITY: SANS REPORT**

HERE ARE SOME ACTIONABLE STEPS TO MATURE YOUR SECURITY AWARENESS PROGRAMS. AND COMPARE YOUR PROGRAM AGAINST GLOBAL BENCHMARKS



ith an unprecedented number of employees now working in hybrid or fully remote environments,

compounded by an increase in cyber threats and a more overwhelmed, COVID-19 information fatigued workforce, there has never been a more critical time to effectively create and maintain a cyber-secure workforce and an engaged security culture.

"People have become the primary attack vector for cyber-attackers around the world," said Lance Spitzner, SANS Security Awareness Director and co-author of the report. "Humans rather than technology represent the

greatest risk to organisations and the professionals who oversee security awareness programs are the key to effectively managing that risk."

After analysing the data of more than 1,000 security awareness professionals worldwide, SANS Security Awareness, the global leader in providing security awareness training, has released its seventh annual SANS Security Awareness Report. The 2022 report establishes updated global benchmarks for how organisations manage their human risk and provides actionable steps to making improvements with key metrics in the Security Awareness Maturity Model Indicators Matrix to measure progress.

"Awareness programs enable security teams to effectively manage their human risk by changing how people think about cybersecurity and help them exhibit secure behaviors, from the Board of Directors on down," said Spitzner. "This report enables security awareness professionals to make data-driven decisions on how to best secure their workforce and speak to leadership about risk in a compelling way that demonstrates value and support for their strategic priorities."

#### **Key Findings:**

• Workforce: More than 69% of security awareness professionals are spending less than half their time on security awareness. The data shows that security awareness responsibilities

are very commonly assigned to staff with highly technical backgrounds who may lack the skills needed to effectively engage their workforce in simple-to-understand terms.

- US Compensation: The average salary reported was \$110,309 USD for security training professionals, an increase from 2021. However, those dedicated full-time to awareness were paid on average only \$86,626, while those who are part-time averaged \$117,584 – \$30,000 difference. This difference is because people dedicated parttime to security awareness have their compensation based on their other responsibilities, which are usually more technically focused.
- Global Compensation: Security awareness professionals in Australia/New Zealand had the highest average annual compensation (\$121,236), while South America had the lowest (\$56,960). In North America, the higher the maturity level of an organization's security awareness program, the higher the salary for the awareness professionals who work there.
- **Top Reported Challenges:** The three top reported challenges for building a mature awareness program were all related to a lack of time: specifically lack of time for project management,

#### THE MOST MATURE SECURITY AWARENESS PROGRAMS NOT ONLY CHANGE THEIR WORKFORCE'S BEHAVIOR AND CULTURE BUT ALSO MEASURE AND DEMONSTRATE THEIR VALUE TO LEADERSHIP VIA A METRICS FRAMEWORK.

limits on training time to engage employees, and a lack of staffing.

- Pandemic Impacts: The top two reported impacts were the challenge of a more distracted and overwhelmed workforce and a working environment where humanbased cyber-attacks have become more frequent and effective.
- Program Maturity by Region: Consistent across all global regions is that current programs' most common maturity levels are compliance-focused and awareness/ behavior change.
- Successful Program Indicators: Strong leadership support, increased team size, and a higher training frequency topped the charts as key enablers to program success.

#### Key Action Items to Increase Program Success:

• Action Items to Increase Leadership Support: One of the top ways to



increase leadership support is speaking in terms of managing risk, not compliance, and explaining WHY you are doing something, not WHAT you are doing. Additionally, creating a sense of urgency by utilising data and communicating value by demonstrating alignment with leadership's priorities.

- Action Items to Increase Team Size: Documenting and contrasting how many people on the security team are focused on technology versus how many on the team are focused on human risk, creating a document to explain personnel needs fully, and developing partnerships with key departments that can help develop ways to communicate the program's value were recommended.
- Action Items to Increase Training Frequency: It is recommended that organisations communicate to, interact with, or train their workforce at least once a month. Keeping training simple and easy to follow is the key to increasing your opportunities to engage and train your workforce.

"The most mature security awareness programs not only change their workforce's behavior and culture but also measure and demonstrate their value to leadership via a metrics framework," Spitzner added. "Organisations can no longer justify an annual training to check the compliance box, and it remains critical for organisations to dedicate enough personnel, resources, and tools to manage their human risk effectively."

# ZERO TRUST, CLOUD & REMOTE WORKING DRIVE DIGITAL RESILIENCY

#### PAUL NICHOLSON, SR. DIRECTOR OF PRODUCT MARKETING AT A10 NETWORKS

WE ARE WITNESSING A BROAD SPECTRUM OF CONCERNS AS ENTERPRISE ORGANISATIONS LOOK TO SHORE UP THEIR DEFENCES oday's enterprises have faced many challenges with the pace of change over the last few years because of digital transformation, and the need for that transformation to be resilient and secure. These challenges have been amplified by the disruption of the global pandemic.

There have been massive global macro-economic shifts that have fundamentally changed the way companies operate, from the rise of remotely working employees to the adjustments of customer engagement strategies. Remote work was in full swing before the pandemic and it already had an impact on IT strategy and the shift to cloud, including hybrid cloud. This trend has only accelerated due to the ease of remote deployment and accessibility for software, SaaS, and cloud options. With all these changes, the specter of security breaches is high. This explains the rise and popularity of Zero Trust as a framework for securing networks in these new realties, and as an effective tool to drive cybersecurity initiatives within the entire enterprise.

All this means that in a post-pandemic era, digital resilience is a top priority and cyber threats are only accelerating. As a result, we are witnessing a broad spectrum of concerns as enterprise organisations look to shore up their defences.

Analysing the events of the last two years, it is an ideal time to explore enterprise perceptions about the future. To gain these insights, we surveyed 2,425 senior application and network professionals from across ten regions around the globe. Not surprisingly, we found high levels of concern around all aspects of digital transformation solutions and resilience with a strong focus on business continuity. The top findings we uncovered included:

#### Private Clouds are the Preferred Enterprise IT Environment

Even though we witnessed a rapid pivot to cloud in the last couple of years, plenty of on-premises environments remain. Twenty-three percent of respondents have retained an onpremises environment and this is unlikely to change in the future. Private clouds were the preferred environment for 30 percent of respondents, while just under one quarter said their environment was in a public cloud with a similar percent in SaaS environments.

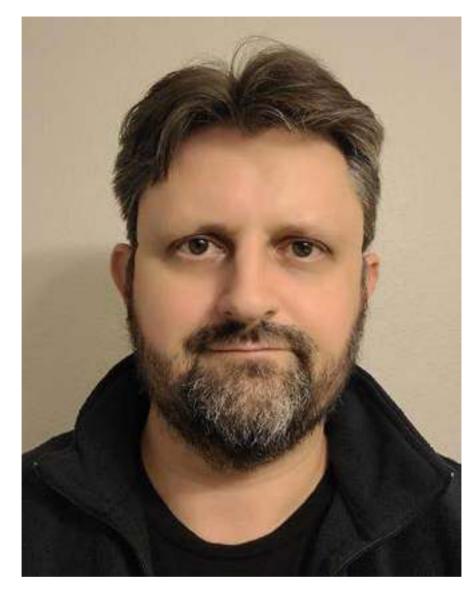
#### New Working Patterns and Digitalisation Prompt Rethinking the Strategy

Resilience is a board-level discussion as senior leaders look to ensure that the business can cope with any future disruption. Our enterprise respondents said that digital transformation solutions, business continuity (technically and organisationally) and stronger security requirements have all become paramount. This puts tremendous pressure on IT professionals to rethink their architectures and IT strategies to meet the challenge.

Asked to rate their concern about 11 different aspects of business resilience, nine out of 10 respondents expressed some level of concern about every issue. The top concerns were around the challenge of optimising security tools to ensure competitive advantage, utilising IT resources in the cloud, and enabling remote access and hybrid working while ensuring that staff feel supported in whatever work style they wish to adopt.

#### Top Cyber Threat Concerns for Enterprise IT

Without a doubt, the escalating threat landscape is causing a broad array



of concerns from respondents. Chief among them is the loss of sensitive assets and data followed by the disruptive impact of downtime or network lockdown. In response, there was an evident shift to a Zero Trust security approach. One-third (30%) of enterprise organisations said that they had already adopted a Zero Trust model.

Looking to the future, we expect adoption of cybersecurity initiatives to not only remain high, but to become higher. This includes a more pervasive adoption of the Zero Trust model within the enterprise as all employees become more aware of the benefits of such a strategy and approach.

It's clear that there is unlikely to be any relief from the pressures for enterprises and their IT practitioners. whether in infrastructure or security domains. We will be dealing with the impact of these recent pandemicrelated changes for years to come, including the continuing integration of newer technologies and evolving standards. Therefore, IT organisations must continue to invest in modern technologies that support ongoing digital transformation initiatives but strike the balance between strong Zero Trust defence and operational agility for their multifaceted digital resiliency needs. 1



# 3 THINGS BUSINESS LEADERS Should know about Security

#### DAVE RUSSELL, VP OF ENTERPRISE STRATEGY, VEEAM SOFTWARE

few years ago, Cathay Pacific suffered a lapse in data security, affecting the personal information of an estimated 9.4 million people. Along with the questions it raised around the effectiveness of cybersecurity for all companies, a top international law firm noted another effect: an uptick in interest in collective redress, a type of representative action resembling a class action lawsuit.

Two years later, cybersecurity would once again step into the spotlight as risk

shot up, in step with millions of people around the world shifting to remote work during the global pandemic. Multiple Asiabased offices of international insurance giant AXA, the Singapore-based arm of Japan-based insurance company Tokio Marine Group, and several military groups throughout Southeast Asia have become just a few of the targets of ransomware attacks within the past year.

Designed to spread through a network, ransomware is malicious software that infects a computer and restricts access to crucial user data for a ransom. The cost of a ransomware attack can amount to nearly US\$2 million per incident and have a global economic impact of over US\$20 billion. Ransomware attacks rose by 93% last year.

As citizens become increasingly acquainted with the value of their data, any negligence, misuse or lack of adequate protection has moved into the spotlight of possible issues for company boards across APJ. With class action and consumer group-led lawsuits on the rise, the responsibility to protect against ransomware and other cyberattacks that threaten user data and privacy has become more critical than ever for businesses.

The other reason that data and privacy have arisen as such crucial topics is timing. A Trend Micro survey found Asia Pacific to be the second-most vulnerable region in the world to cyberattacks, after North America. Ransomware attacks ranked in the top five cyber threats in the region, while confidence in company preparedness lagged: a staggering 86% of survey respondents believed they would be breached in the next 12 months.

In the wake of this information, business leaders should sit up and take notice: data breaches are no longer an issue that exists within a company itself – they sit at the board level as well. Moving forward, business leaders should expect increasing momentum toward ensuring the right cybersecurity measures are in place.

Here are three things to keep in focus when implementing security measures.

1. Emphasise the importance of cybersecurity training for all

Ransomware has the ability to spread through a system like wildfire, but it needs an entry point, such as an infected email, email attachment, or application. No matter their role, any member of an organisation has the ability to lead the ransomware into the system.

Thorough, regular, up-to-date trainings on best cybersecurity practices are the best preventative measure to keeping systems and profits safe, so make sure the company's cybersecurity plan affords it the resources it needs.

### 2. Keep anti-virus and malware software updated

Up-to-date anti-virus and malware software can help catch and eliminate



the most common ransomware payloads. Like any software, it needs frequent updates, but if used correctly, it can keep your business' systems clean with minimal downtime and interruptions.

#### 3. Have a secure backup ready

If protections happen to fail and a business finds itself dealing with a ransomware attack, one can gain access to a system again by restoring it from a

MOVING FORWARD, BUSINESS LEADERS SHOULD EXPECT INCREASING MOMENTUM TOWARD ENSURING THAT THE RIGHT CYBERSECURITY MEASURES ARE IN PLACE. secure and reliable backup, saving the business from downtime, data loss and an often-expensive ransom. Veeam's ransomware protection, for example, can restore a business' data and system while adhering to compliance standards, with real time updates and alerts. Before restoring the system, the backup scans files for malware and provides flexible storage options for a range of files.

Ransomware attacks are much more a possibility than they used to be, but they don't have to cost the business significant portions of its profits. With the right cybersecurity infrastructure and training in place, companies can sufficiently prepare and defend themselves against these breaches moving forward.



# WOMEN IN CYBERSECURITY

**DEEPA KUPPUSWAMY,** INFORMATION SECURITY ARCHITECT, MANAGEENGINE TELLS ANITA JOSEPH ALL ABOUT THE CHANGING ROLE OF WOMEN IN THE SECURITY SPACE.

#### ell us about the role of women in cybersecurity and how it has evolved with time.

Several cryptographic and computer science milestones have been pioneered by women, with many of their contributions being ignored or downplayed. There's always been an under-representation of women in the tech field, especially cybersecurity. According to Cybersecurity Ventures, one in four cybersecurity roles globally are filled by women, which is too low.

Although there have been efforts to increase the involvement of women in cybersecurity and other STEM roles, many long-standing social norms continue to shape public perception. Despite these challenges, the industry is currently facing a huge skills gap. The need to hire talent irrespective of their gender and other background details is becoming more significant than ever. So, ideally, we'll see more women in cybersecurity roles in the coming years. CYBERSECURITY WORKERS ARE OFTEN DEPICTED AS HOODIE-WEARING MEN WHO SIT IN FRONT OF COMPUTER → SCREENS ALL DAY AND HACK SYSTEMS.

#### What, in your opinion, is the biggest challenge for women when it comes to take up security/cybersecurity-related roles?

The biggest deterrent is the stereotyping of the industry. Cybersecurity workers are often depicted as hoodie-wearing men who sit in front of computer screens all day and hack systems. Roles in the industry are often portrayed as taking place in high-stress environments with cutthroat competition. This creates a negative, unwelcome perception that can deter women from entering the cybersecurity field unless they have a strong personality (which can trigger negative stereotypes about them) or have been dispelled of these stereotypes.

#### What do you think can be done, to make global workplaces more inclusive and women-friendly?

Organisations can make cybersecurity more inclusive by implementing best practices that specifically address issues women face. Tackling preconceived notions that recruiters have while hiring women and avoiding the age-old question of work-life balance that all women face is a good place to start. This goes both ways. Some aspirants have a similar prejudice when it comes to the roles they believe they qualify and would



be considered for in the cybersecurity field. It is the joint responsibility of organizations and academic institutions that educate and train the candidates who constitute the workforce to properly set expectations that women can and should participate in the cybersecurity industry.

# What would be your advice to women wishing to take up roles in the security domain?

Cybersecurity is a dynamic field requiring constant learning and upskilling. There

is a need to stay up to date with industry developments. I'd encourage women to be keen learners and embrace new challenges. An important aspect is taking ownership of their career path, focusing on excellence in execution and communicating their expertise from a position of confidence. Another focus area that shouldn't be overlooked is the cultivation of a strong peer network at all levels, which offers opportunities for learning new technologies and encountering descriptions of real-world problems. **1** 

#### FINAL WORD / CYBEREASON



# CYBEREASON WARNS AGAINST DESTRUCTIVE RANSOMWARE ATTACKS

Lior Div

vbereason, the XDR company, has issued a global threat alert advisory warning global organisations about a rise in ransomware attacks from the Black Basta gang. The Black Basta gang emerged in April 2022 and has victimised nearly 50 companies in the United States, United Kingdom, Australia, New Zealand and Canada. Organisations in English speaking countries appear to be targets. Cybereason assesses the threat level of ransomware attacks against global organisations today being HIGHLY SEVERE.

"Since Black Basta is relatively new, not a lot is known about the group. Due to their rapid ascension and the precision of their attacks, Black Basta is likely operated by former members of the defunct Conti and REvil gangs, the two most profitable ransomware gangs in 2021," said Lior Div, Cybereason CEO & Co-founder.

Black Basta has been using the double extortion scheme on their victims and

some of their ransom demands have exceeded \$1 million. Double extortion works when attackers penetrate a victim's network, steal sensitive information by moving laterally through organisations and threaten to publish the stolen data unless the ransom demand is paid.

Cybereason offers these recommendations to organisations to reduce their risks:

- Practicing good security hygiene like implementing a security awareness program for employees, assuring operating systems and other software are regularly updated and patched.
- Assuring key players can be reached at any time of day as critical response actions can be delayed during holidays and when attacks occur during off hours and on weekends and holidays.
- Conducting periodic table-top exercises and drills and including those beyond the security team like Legal, Human Resources, IT Support and all the way up to the Executive

BLACK BASTA HAS BEEN USING THE DOUBLE EXTORTION SCHEME ON THEIR VICTIMS AND SOME OF THEIR RANSOM DEMANDS HAVE EXCEEDED \$1 MILLION. Suite is also key to running a smooth incident response.

- Ensuring clear isolation practices are in place to stop any further ingress on the network or spreading of the ransomware to other devices. Teams should be proficient at things like disconnecting a host, locking down a compromised account, and blocking a malicious domain, etc. Testing these procedures with scheduled or unscheduled drills at least every guarter is recommended.
- Evaluating lock-down of critical accounts when possible. The path attackers often take in propagating ransomware across a network is to escalate privileges to the admin domain-level and then deploy the ransomware. Teams should create highly secured, emergency-only accounts in the active directory that are only used when other operational accounts are temporarily disabled as a precaution or inaccessible during a ransomware attack.
- Deploying EDR on all endpoints. The quickest remedy to the ransomware scourge for public and private sector businesses is deploying EDR on endpoints according to Gartner's Peter Firstbrook. Yet Firstbrook says that only 40 percent of endpoints have EDR. 1

# **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.



بر الم 4





**4**G





Scan to Learn More

HIKVISIONMENA in HIKVISION-MENA

(O) HIKVISIONMENA D HIKVISIONMENA

21. 首席 16年





# EVERDOME

# The Digital Frontier's First Hyper-realistic #Metaverse

Everdome aims to create the most hyper-realistic metaverse that will bring brands and people together - all with the intent of building the most realistic web3 experience.

See whats waiting for you...

everdome.io