Sec

**ADVISOR** 

## HIGHLIGHTS MMA INFOSEC-eSENTIRE AXON TECHNOLOGIES SOPHOS

MIDDLE EAST

# THE COMPLETE PICTURE

GOPAN SIVASANKARAN, GENERAL MANAGER META AT SECUREWORKS, ON WHY IT'S IMPORTANT TO ADOPT A HOLISTIC APPROACH TO SECURITY.

🛞 tahawultech.com







## Unlimited Devices. Unlimited Networks. Unlimited Possibilities.

Remotely Manage Your Access Points Through The Cloud

Outdoor 1300AC WiFi 5 MU-MIMO Cloud Managed Wireless Access Point LAPAC1300CE

The Linksys LAPAC1300CE delivers 802.11AC Wave 2 MU-MIMO WiFi 5 technology to provide data rates up to 1300 Mbps and includes Linksys Cloud Manager 2.0 for remote management or Zero Touch Provisioning.

- Dual-Band 802.11AC Wave 2 MU-MIMO (2.4GHz + 5GHz)
- 2x2:2 for AC1300 Speeds (400Mbps + 867Mbps)
- Four (4) Removable Antennas (SMA)
- IP67 Rated for Outdoor Applications

- 802.3af/at PoE or PoE+ Support
- Limited Lifetime Cloud Management
- TAA Compliant

## **Linksys Managed Gigabit Switches**

As your business network grows, you may require a more sophisticated system to securely handle increased traffic loads. Our LGS300 Series managed switches offer you even more control over data streams so you can minimize network traffic jams and mitigate security risks.

#### LGS310C 8-port LGS328C 24-Port LGS352C 48-Port





Advanced QoS (per-flow) features ensure the proper prioritization of traffic to deliver the best possible user experience.



Port authentication along with advanced DHCP snooping and IP-MAC-Port binding protect your network and data. 10 GB

1G SFP and 10G SFP+ Uplinks

Speed up your network with dedicated SFP/SFP+ uplinks back to your core.

# CONTENTS

# 





# THE COMPLET PICTURE

Gopan Sivasankaran, General Manager META at Secureworks, on why it's important to adopt a holistic approach to security.

# 06 News

News roundup from the cybersecurity industry in the region.

**18** Harish Chib, Vice-President, Middle East & Africa at Sophos, on threat & security landscape in 2022, the ever-growing popularity of Ransomware as the attack of choice, and the role that AI is playing in cybersecurity. 28 Rick Peters, CISO Operational Technology at Fortinet, on how OT cyber events have demonstrated the consequence of failing to invest and commit proportionally to a cybersecurity strategy.

40 Saket Modi, Co-Founder and CEO at Safe Security, on how cybersecurity must be aligned in every organization driven by products that deliver holistic and actionable insights.



# Bedata 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



## EDITORIAL



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

> Anita Joseph Editor

#### **EVENTS**



# **STARTING AFRESH**

#### 2022 began on a cautious note.

Particularly on the cybersecurity front, there was and continues to be a shadow of uncertainty, as the threats of 2021 continue unabated and bigger and bolder ones are anticipated.

To add to this, the complexities brought on by remote working have heightened the anxiety, as decision makers face tough decisions on how to provide the same level of security that used to be taken for granted when work was completely physical.

So, 2022 looks to be a mixed bag for the security industry. However, it's clear that a complete overhaul of existing security measures is necessary if the ever-

growing threat landscape is to be dealt with firmly and effectively.

This issue of Security Advisor brings you exclusive inputs from the who's-who of the cybersecurity industry, about the trends to watch out for this year. From predictive analysis to zero trust to threat intelligence, the approaches are many and varied. And as the Cloud continues to hold sway, things become more diverse and intense. We have a special interview with David Brown, Security Operations Director, Abed Samhuri, Cyber Institute Lead and Andrew Schumer, Technical Director at Axon Technologies, who discuss tactics for effective cyber defence, the importance of gamification in cybersecurity and the company's plans for 2022.

We also have Piers Morgan - GM Sales EMEA, eSentire and Amit Kumar, Managing Director MMA InfoSec, talk about tapping into the potential of MDR in the region

2022 LOOKS TO BE A MIXED BAG FOR THE CYBERSECURITY INDUSTRY. and the comprehensive partnership between both companies for a comprehensive and cuttingedge approach to risk. Phil Muncaster from ESET gives

us ten cybersecurity habits to shed in 2022-these include scrapping outdated software to ramping up password hygiene.

In addition, we have the regular News Roundup, Perspective and Security Matters columns, which bring fresh insight and information in a year that promises to be exciting and action-packed. So, here's to new beginnings, Happy Reading!



Registered at Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Reception: +971 4 5682993 Operations: +971 4 5682994 Accounts: +971 4 5682995

© 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.

FOUNDER, CPI MEDIA GROUP Dominic De Sousa (1959-2015)

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

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

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com EDITORIAL Editor Anita Joseph anita.ioseph@cpimediagroup.com

Online Editor Daniel Shepherd daniel.shepherd@cpimediagroup.com DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com

> DIGITAL SERVICES Web Developer Adarsh Snehajan

# STARLINK & ANOMALI PARTNER FOR INNOVATIVE THREAT DETECTION & RESPONSE SOLUTIONS



ZAIDOUN ARBAD, COO, STARLINK & JUSTIN COKER, VICE PRESIDENT AND GENERAL MANAGER OF EUROPE AND THE MIDDLE EAST (EMEA), ANOMALI.

#### StarLink, the fastest growing Cyber and

Cloud Advisor in the META region, has announced a distribution partnership with Anomali, the leader in intelligence-driven extended detection and response (XDR) cybersecurity solutions. By adding Anomali to its portfolio, joint customers' security teams will gain in-depth visibility over all threats, automate threat blocking, and enable faster response times. This new partnership will provide organisations across MEA with access to the awardwinning Anomali portfolio, an innovative suite of products that leverages global intelligence to empower security teams with the precision attack detection and optimised response needed to stop immediate and future breaches and attackers.

"In a time where we are experiencing rapid expansion of the threat landscape globally, where cyber threats can have major repercussions on businesses, it is imperative to replace reactive remediation with proactive detection and response to ensure seamless operations and optimum returns on security investments", commented Zaidoun Arbad, COO, StarLink. "StarLink and Anomali will jointly empower enterprises to up their defences with timely threat intelligence so they can stay on top of the latest cyber threats and achieve effective and efficient cyber resilience", He added.

"Advanced adversaries are launching a relentless level of cyberattacks against public and private sector organisations across the Middle East. A lack of threat detection and response solutions coupled with talent shortages is leaving many security teams at a disadvantage when it comes to defending against advanced adversaries", said Justin Coker, Vice President and General Manager of Europe and the Middle East (EMEA), Anomali. "As part of our commitment to helping organisations around the world build and maintain resilient cybersecurity postures, we are providing partners like StarLink with valuable benefits, incentives, and support needed to reach vast markets that are demanding new levels of efficient and effective security products and services".

# MIMECAST NAMED 2021 SOFTWAREREVIEWS CHAMPION IN SECURE EMAIL GATEWAY AND DATA ARCHIVING CATEGORIES

#### Mimecast Limited, a

leading email security and cyber resilience company, has announced it has been named a 2021 SoftwareReviews Champion in two categories: Secure Email Gateway - Enterprise and Data Archiving. SoftwareReviews, a peer review platform, is a leading source of expertise and insight into the

of expertise and insight into the enterprise software landscape and client-vendor relationships.



Mimecast Email Security with Targeted Threat Protection and Mimecast® Cloud Archive were recognized as an Emotional Footprint Champion in their respective 2021 SoftwareReviews Reports. For Emotional Footprint Reports, SoftwareReviews evaluates 27 aspects of the customer relationship

using a net promoter methodology. These ratings include detailed questions on the experience of working with the vendor, creating a powerful indicator of overall user sentiment.

"The vendor relationship, what we call the Emotional Footprint, has never mattered more than during the pandemic," said David Piazza, president, Software Reviews. "Over the past year, the gap between top and bottom-ranked vendors grew by 25% as organizations honed-in on the vendors that provided the most value and exhibited the most flexibility with their services. We expect this upward trend to continue as the pandemic highlighted which vendors rose to the occasion to support their customers."

## SOPHOS PREMIERS SOPHOS SWITCH SERIES TO STRENGTHEN AND SIMPLIFY CONNECTIVITY AT THE ACCESS LAYER

#### Sophos, a global leader in next-

generation cybersecurity, has unveiled the Sophos Switch Series, featuring a range of network access layer switches to connect, power and control device access within a Local Area Network (LAN). The new offering adds another component to Sophos' secure access portfolio, which also includes Sophos Firewall and Sophos Wireless.

"Sophos Switch seamlessly integrates with the Sophos adaptive cybersecurity ecosystem to extend connectivity across office LANs," said Joe Levy, chief technology officer at Sophos. "We're removing the complexities of multi-vendor deployments by providing organizations and channel partners with a single source of management, monitoring and troubleshooting."

Switches are remotely managed in the cloud-based Sophos Central platform. This enables partners to oversee all customer installations, respond to alerts, and track licenses and upcoming renewal dates via a single, intuitive interface.

"Sophos Switch perfectly complements the existing Sophos portfolio – it was the missing piece in our IT security offering, and now gives our business even more clout. We were already very successful with Sophos Firewall, and thanks to Sophos Switch we are now able to unleash the full power of Sophos' products and services. Our experience from the early access JOE LEVY

program proved that Sophos Switch is a game changer for us, and we were very positively surprised at how well the product worked from day one," said Patrizio Perret, chief technology officer at Avanet. "While a switch is pretty much a commodity these days, Sophos is adding the necessary spice to the hardware with the software capabilities. Sophos' adaptive cybersecurity ecosystem is the magic ingredient that will make Sophos Switch something really special by enabling companies to integrate it with other Sophos security components in their network."

## ZOOM BECOMES FIRST VIDEO COMMUNICATIONS CLIENT TO ATTAIN COMMON CRITERIA CERTIFICATION

COMMON CRITERIA I

ΔΝ INTERNATIONAL

STANDARD FOR

SATISFIES A DEFINED

**REQUIREMENTS.** 

**SET OF SECURI** 

**Zoom Video Communications, Inc.** has announced that Zoom Meeting Client version 5.6.6 has become the first video communications client to attain certification for Common Criteria Evaluation Assurance Level 2 (v3.1 rev. 5), issued by the German Federal Office for Information Security (BSI).

Common Criteria is an international standard for objectively evaluating that an IT product satisfies a defined set of security requirements. The evaluation involves analyzing a specific set of security targets, including guidance documentation, architectural design, life cycle aspects, testing and vulnerability assessment. The Zoom Meeting Client v5.6.6 has been evaluated by the BSI against the Common Criteria standard and found to exhibit a clear chain of evidence that the process of specification, implementation, and

> evaluation has been conducted in a rigorous and standard manner.

"This Common Criteria certification represents a major milestone for Zoom," said Jason Lee, Chief Information Security Officer at Zoom. "We're JASON LEE



the first video communications client to receive this important certification, reinforcing our commitment to our customers. Security and privacy are the cornerstones of everything we do, and we are continually innovating secure solutions for all users of our platform."

At present, the BSI has certified Zoom version 5.6.6 for Windows, macOS, iOS, and Android. While version 5.6.6 was the version of Zoom client available at the time of the certification, we always recommend customers utilize the newest version of the client to take advantage of Zoom's latest security updates and features.

## ACRONIS APPOINTS MICHAEL CALLAHAN AS CHIEF MARKETING OFFICER

MICHAEL CALLAHAN



#### Acronis,

a global leader in cyber protection.

has announced the appointment of Michael Callahan as its new Chief Marketing Officer. Callahan joins the team with extensive sales and marketing experience, serving in senior leadership roles at companies such as McAfee, HP, and Juniper, and most recently as the Senior Vice President of Global Marketing for Cofense.

As Acronis' Chief Marketing Officer, Callahan will develop Acronis' global brand position while increasing awareness of the Cyber Protect Cloud Platform. With COVID-19 accelerating digital transformation solutions and the migration to cloud and hybrid solutions, organizations need an effective security solution to stop the always-evolving threats. In addition, Callahan will help expand Acronis' dedication to nurturing the next group of tech leaders with outreach programs around the world, especially in disadvantaged areas.

Callahan is a metrics-driven marketing executive with extensive software-as-aservice (SaaS) security domain experience, serving in leadership roles at McAfee, HP, Firemon and Zimperium, where he effectively managed and led global teams. This is essential experience for this position as Acronis prides itself on being an internationally connected company with offices and employees around the globe, enabling the company to reach broader demographics and extend its grasp on the cyber protection markets.

## KASPERSKY NAMED A MAJOR PLAYER IN MODERN ENDPOINT SECURITY FOR ENTERPRISE AND SMB BY IDC MARKETSCAPE

Kaspersky was recently named a Major Player in the IDC MarketScape reports for 'Worldwide Modern Endpoint Security for Small and Midsize Businesses 2021 Vendor Assessment' (Doc #US48304721) and 'Worldwide Modern Endpoint Security for Enterprises 2021 Vendor Assessment' (Doc #US48306021).

The recognition is testament to the breadth and quality of products, services and training solutions that Kaspersky offers its corporate customers.

To help organizations evaluate the best endpoint protection platforms (EPP) and endpoint detection and response (EDR) solutions for their needs, the IDC MarketScape reviewed data submitted by MES vendors (22 SMBs and 19 enterprises) between April and EVGENIYA NAUMOVA

September 2021, to position the capabilities of the companies.

"It has always been our mission to help our customers protect themselves from evolving threats. This recognition by IDC MarketScape serves to underpin our work and the continued investment we make in our solutions to support businesses of all sizes. Every organization has different needs when it comes to security and these comprehensive IDC MarketScape vendor evaluation reports provide an independent view on the solutions available," said Evgeniya Naumova, Executive VP Corporate Business at Kaspersky.

## FINESSE JOINS HANDS WITH BARRACUDA FOR CLOUD-ENABLED SECURITY SOLUTIONS



Finesse has entered into an agreement with Barracuda, a leading provider for cloud-enabled security solutions, to provide its customers with easy-to-deploy cloud security solutions. Through this agreement, Finesse's expertise in digital transformation will be complemented by the power and simplicity of Barracuda's cybersecurity solutions portfolio, enabling Finesse customers to reduce cybersecurity risk on their digital journeys.

"We are excited to add Barracuda's

 portfolio," said Shahanavas Mohammed Shafi – Business
PIN Development Manager. "Finesse is dedicated to ensuring our customers have access to the latest and most secure technology. Barracuda

is a global leader in cybersecurity, their products will help our customers with the tools and expertise to safeguard their employees, data, and applications from a wide range of threats."

"With their expertise as a trusted digital transformation partner to the most prominent regional enterprises, Finesse is perfectly positioned to empower its customers to realise the full potential of Barracuda's market-leading cybersecurity solutions," said Chris Ross, SVP International Sales, at Barracuda.

## NETAPP ONTAP BECOMES FIRST ENTERPRISE **STORAGE PLATFORM TO RECEIVE VALIDATION** FROM NSA FOR SECURITY & ENCRYPTION

NetApp, a global, cloud-led, data-centric software company, has announced that NetApp ONTAP, the world's leading storage operating system, is the first enterprise storage and data management platform to achieve Commercial Solutions for Classified (CSfC) validation for a data-at-rest (DAR) capability package. With this, organizations across the globe can benefit from NetApp ONTAP's robust security capabilities to protect customers' information onpremises and in remote locations from foreign actors, ransomware attacks or other data loss threats they may face.

A cybersecurity program led by the U.S. National Security Agency (NSA), CSfC is

a key component of the organization's commercial cybersecurity strategy. CSfC validates commercial IT products that have met the highest level of strict encryption standards and rigorous security requirements for both hardware and software solutions. Recently, the NSA has recommended that federal agencies hosting secret or top-secret data utilize storage solutions that have been CSfC validated.

"This unique achievement is an example of innovation in commercial technology addressing critical national security issues," said Admiral Michael S. Rogers USN (Ret.), former Director, National Security Agency (NSA) and Chief, Central Security Service (CSS).



MICHELLE RUDNICKI

"Organizations today know that data security is paramount, whether they operate in the public or private sector," said Michelle Rudnicki, Vice President, US Public Sector at NetApp. "With NetApp's world-class data security capabilities and this CSfC validation, government organizations as well as companies in highly regulated industries like financial services. healthcare. energy or any organization with valuable intellectual property can be reassured that their most sensitive data is secure with NetApp ONTAP."

## QUANTUM EXTENDS VIDEO SURVEILLANCE OFFERINGS **ACROSS MIDDLE EAST & AFRICA WITH MOBIUS**



ALI YARMOHAMMADI

#### Quantum has signalled its agreement

with leading value-added distributor (VAD) Mobius to deliver the industry's broadest security and video surveillance infrastructure portfolio available from any single vendor, across the Middle East and Africa regions (MEA).

The partnership allows Mobius, the



ANAND CHAKRAVARTHI

leading emerging distributor within the video surveillance market in MEA. to now offer customers Quantum's entire security infrastructure portfolio, from high-performance NVRs, to hyperconverged infrastructure (HCI), to the largest shared storage and archive solutions, and analytics processing.

"The availability of Quantum's video surveillance offerings is a welcome addition to our top-class vendor portfolio," said Ali Yarmohammadi, Managing Director at Mobius MEA. "For the past 20 years we've invested in creating an environment for security enthusiasts to innovate, collaborate and engage in complex projects. Bringing Quantum onboard means that we can continue to stay true to that vision and provide our customers with the best available solutions in the market."

"We are excited to partner with an industry leader like Mobius. This agreement substantially extends Quantum's footprint across a key region and opens an essential sales channel to customers looking for purpose-built, end-to-end video surveillance solutions to store, manage, protect and enrich their video data," said Anand Chakravarthi, Director - Strategic Markets, EMEA and South Asia at Quantum.

# PARTNERING FOR GREATER SECURITY

**PIERS MORGAN** - GM SALES EMEA, **ESENTIRE** & **AMIT KUMAR**, MANAGING DIRECTOR, **MMA INFOSEC**, SPEAK TO **ANITA JOSEPH**, EDITOR, SECURITY ADVISOR MIDDLE EAST, ABOUT TAPPING INTO THE POTENTIAL OF MDR IN THE REGION AND THE PARTNERSHIP BETWEEN BOTH COMPANIES FOR A COMPREHENSIVE AND CUTTING-EDGE APPROACH TO RISK.

hat is the role of MMA Infosec in harnessing the potential of MDR? Amit: According to

Gartner, "security and risk management leaders responsible for security operations should use MDR services to obtain 24/7, remotely delivered modern security operations centre capabilities when there are no existing internal capabilities, or when the organisation needs to accelerate or augment existing security operations capabilities."

MMA Infosec, with its partnership with eSentire is at the heart of it. With many years of experience in the cyber security & IT industry, the team at MMA Infosec is well equipped in addressing the agile needs of customers today & helping them plan better for tomorrow. MDR is the future indeed and with our perseverance, our aim is to educate customers to be ready for embracing this technology well in advance with their trusted MDR providers, MMA Infosec.

#### Can you outline MMA's plans for 2022?

Our aim is to be a \$2 million company by end of 2022 by not just adding value for more & more customers across all industries, but also adding niche vendors to our portfolio, with eSentire at the heart of it. Customer retention & customer success are two important values that will fuel this growth, of course, in pursuit of excellence.

#### Please tell us about the growth and business outlook for eSentire

**Piers:** Initially, eSentire's Managed Detection and Response (MDR) business was developed in North America. However, we are currently scaling at 100%+ growth Quarter over Quarter across the UK, EMEA, and the rest of the world, including Asia Pacific and the UAE region specifically.

• Between eSentire's MDR business and our new Emergency Incident Response and Digital Forensics services, which makes a 4-hour, remote threat suppression SLA available to organizations globally, eSentire will surpass \$100M in Annual Recurring Revenue (ARR) this fiscal year.

• eSentire protects the critical data and applications of over 1000 customers, in over 70 countries globally

• eSentire has 2 global 24/7 Security Operation Centers (SOCs) operating in Cork Ireland, and Waterloo Canada.

• eSentire ingests over 20M security signals daily, blocks 3M cyberthreats automatically with our Extended Detection and Response (XDR) platform—Atlas. eSentire's has a Mean Time to Contain threats of 15 minutes.

## What type of commitment will we see from eSentire to the UAE region?

**Piers:** Partners like MMA Infosec are a critical component of our go- to- market

motion. Our partners are an extension of our internal team. MMA InfoSec's customers look to them as their trusted security advisor. And combining our market-leading MDR services and MMA InfoSec's proven security solutions, we are able to protect MMA's customers' from business-disrupting attacks.

b. eSentire works with the top ISVs in the industry.

• As a Microsoft Microsoft Gold Security Partner, eSentire's MDR services are fully integrated with the Microsoft 365 Defender and Azure Defender Product Suites providing Microsoft customers with 24/7 Threat Detection, Containment and Response

• eSentire has been awarded the AWS Level 1 Managed Security Service Provider Competency Status

• eSentire has integrated its MDR services with top ISVs including CrowdStrike, Carbon Black, Sumo Logic and Tenable, so our partners have the industry's best security services available to offer to their customers. eSentire has built its MDR Services to that they are easy to implement and can scale when needed so our partners can protect all size customers, no matter if they are large enterprises or small and mid-size organisations.

#### What are some of the top cyber threats eSentire is tracking and disrupting on behalf of its global customers:





Piers: Ransomware-as-a-Service - The Balto-Slavic Cybercrime Culture has produced dozens of ransomware groups; however, distinction between them is blurry. You often hear "this threat group has associated with that group, who has associations with this threat group, who has associations with that threat group". The highly connected nature of Balt-Slavic Cybercrime Culture is an indicator of an evolved cybercrime market. This market specialized in performing and monetizing intrusions, largely through various means of extortion. Ransomware, data theft, and reputation damage are the primary leverage points that these groups apply to their victims. eSentire has been tracking the top ransomware groups since the Fall of 2020, including such infamous groups as REvil/Sodinokibi (disrupted by law enforcement), DarkSide/Black Matter (ceased operations currently), Clop (disrupted by law enforcement), Conti/Ryuk (one of the leading ransomware groups that continues to operate-has shifted from targeting critical infrastructure organisations in the U.S. to targets in the U.K., Europe, Canada and South America.

Some of the top sectors targeted by ransomware threat groups is healthcare, municipalities, manufacturing, organisations serving in critical infrastructure sectors and

#### law firms. Business Email Compromise –

Business Email Compromise (BEC) leverages partnership trust through email communications. In many of the current BEC incidents, many times the attack originates from an email from a business partner. It was often found that the business partner had themselves been the victim of remote exploitation on their Exchange server, and the business partner's email credentials have been hijacked by the threat actors.

This BEC-based approach allows threat actors to bypass email filters and user awareness, given the trusted nature of the business relationship. The lesson here is that even the compromise of one of your partners can provide an initial access vector into your organization.

#### Remote exploits of vulnerable software

"PARTNERS LIKE MMA INFOSEC ARE A CRITICAL COMPONENT OF OUR GO- TO- MARKET MOTION. OUR PARTNERS ARE AN EXTENSION OF OUR INTERNAL TEAM."

#### applications or tools (Kaseya, SolarWinds)-

Used by both financially-motivated cybercriminals and nation-states, remote exploitation is increasingly becoming a regular risk to organisations. As a distributed work force adapts to pandemic policy, organisations are adding more software to their stack. With more software comes more vulnerabilities, and visibility gaps start to form. Meanwhile, the cybercrime market is differentiating and specialists are emerging.

Some of these specialists focus on developing exploits and the discovery of zeroday vulnerabilities. In 2021, we have reached an all-time high of 66 zero-day attacks – over double that of previous years. Detecting zero-days is hard – sometimes impossible. But with endpoint monitoring in place, your chance of catching the actions immediately following exploitation are greatly increased, especially if your security defenders are actively developing your rule set for escalating endpoint alerts.

UAE has announced the adoption of cybersecurity standards for government agencies, and it revealed the cybersecurity budget for the next five years (2022-2026), which is the largest in the history of the Gulf state. This is evidence that the government of the United Arab Emirates is taking cybersecurity protections of its country and its organisations extremely seriously. **1** 

# SAUDI BUSINESSES EXPOSED BY RISKY REMOTE EMPLOYEE BEHAVIOUR

THE STUDY, COMMISSIONED BY TENABLE AND CONDUCTED BY FORRESTER CONSULTING, HIGHLIGHTS THE RISKS INTRODUCED FROM EMPLOYEES WHEN WORKING REMOTELY.

recent study, commissioned by Tenable and conducted by Forrester Consulting, has highlighted the risks introduced from employees when working remotely. The data is drawn from 'Beyond Boundaries: The Future of Cybersecurity in the New World of Work,' a commissioned study of more than 1,300 security leaders, business executives and remote employees, including 104\* respondents in the Kingdom of Saudi Arabia.

David Cumm

When asked how confident security leaders and business executives were that employees were taking adequate measures to protect the organization's data 47% said they were very or completely confident. However, speaking with remote employees showed a different picture.

When asked what was important to them, 85% of remote employees said protecting customer data was somewhat or very important. However, 54% of remote employees reported using a personal device to access this information. It's a similar situation with protecting the organization's intellectual property as 68% of remote employees said it was important while 20% will use a personal device to access it. In fact, just 47% of remote employees said they consistently follow measures to protect their organization's data, intellectual property and systems when working from home.

Digging deeper, just 11% of remote employees strictly follow their organizations' mandates restricting access to data and systems via personal devices. Perhaps most worrying is that 34% of employees said they will ignore or circumvent their organization's

EMPLOYEES WANT THE FLEXIBILITY TO WORK FROM ANYWHERE. THE CHALLENGE IS HOW THEY DO THAT SECURELY." cybersecurity policies, while 21% said one of the challenges they faced is that their organization's security policies and practices weren't clear.

"Employees want the flexibility to work from anywhere. The challenge is how they do that securely," said David Cummins, VP of EMEA at Tenable. "This study confirms what we already suspect remote employees are connecting to sensitive corporate information from personal devices on insecure consumergrade home networks, whether they should or not. Security teams need to accept this reality and change their perception of risk. They require visibility of their entire threat landscape, with the intelligence to predict which cyberthreats will have the greatest business impact on the organization. In tandem, they need to implement adaptive user risk profiles in order to continuously monitor and verify every attempt to access corporate data with the ability to decline requests that fail to meet the rules set."

\* of total respondents, 47 were fulltime employees working from home three or more days a week. **1** 

# 

Russia has a powerful cybersecurity industry. We are No.1 in strong authentication, electronic signature and software protection domains.

Create a secure cryptographic environment at the state level for the exchange of essential information.



Strong authentication and electronic signature



Software monetization and protection against reverse-engineering



Consulting and training in cybersecurity

## Be sure you are protected





aktiv-company.com

global.guardant.com



IT IS A PRIORITY FOR US TO CLEARLY ARTICULATE THE VALUE OF SECUREWORKS WITH TAEGIS AS A HOLISTIC SOLUTION DESIGNED TO HELP CUSTOMERS NAVIGATE THIS COMPLEX LANDSCAPE.

 $\leftarrow$ 

**Gopan Sivasankaran** General Manager META at Secureworks

# THE COMPLETE DICTURE

SECUREWORKS® IS AN UNDISPUTED LEADER IN CUTTING-EDGE CYBERSECURITY SOLUTIONS THAT PROVIDES COMPREHENSIVE PROTECTION AGAINST THE CONTINUOUSLY EVOLVING THREAT LANDSCAPE. IT PROTECTS ORGANISATIONS BY PROVIDING BATTLE-TESTED CYBERSECURITY SOLUTIONS THAT HELP REDUCE RISK, OPTIMISE IT AND SECURITY INVESTMENTS, AND FILL CUSTOMER TALENT GAPS. SECUREWORKS DELIVERS SOLUTIONS BY SECURITY EXPERTS FOR SECURITY EXPERTS, TO HELP PREVENT, DETECT AND RESPOND TO CONTINUOUSLY EVOLVING AND DIVERSIFYING THREATS AND VULNERABILITIES. SECUREWORKS PRODUCTS ARE BUILT ON THE TAEGIS™ CLOUD-NATIVE SECURITY PLATFORM THAT CONTINUOUSLY GATHERS AND INTERPRETS TELEMETRY FROM PROPRIETARY AND 3RD PARTY SOURCES, INCLUDING ENDPOINTS, NETWORKS, CLOUD AND IDENTITY SYSTEMS. THROUGH A COMBINATION OF MACHINE LEARNING AND HUMAN INTELLIGENCE, SECUREWORKS USES THIS TELEMETRY TO HELP DETECT AND PREVENT THREATS, AUTOMATICALLY PRIORITISING THE MOST SERIOUS ISSUES AND ENABLING FASTER, MORE CONFIDENT RESPONSES WITH TIME AND COST-SAVING AUTOMATION.

THE COMPANY, WHICH HAS CHARTED AN ENVIABLE GROWTH TRAJECTORY GLOBALLY AND BUILT UP AN EVER-GROWING CUSTOMER BASE, HAS ALSO MANAGED TO CONSOLIDATE ITS REGIONAL PRESENCE WITH THE RECENT APPOINTMENT OF **GOPAN SIVASANKARAN,** A CYBERSECURITY INDUSTRY VETERAN, AS ITS GENERAL MANAGER FOR THE META REGION. GOPAN LEADS A HIGHLY SKILLED AND DIVERSE TEAM THAT CONTINUES TO GARNER ALL-ROUND APPLAUSE FOR EXCEPTIONAL SERVICE AND PIONEERING SOLUTIONS.

IN AN EXCLUSIVE INTERVIEW, HE TELLS ANITA JOSEPH, EDITOR, SECURITY ADVISOR, THAT THE TIME HAS COME TO ABANDON ALL OUTMODED APPROACHES TO SECURITY AND ADOPT A HOLISTIC FRAMEWORK THAT INCORPORATES CUTTING-EDGE PREPARATION, PREVENTION, DETECTION, RESPONSE AND RECOVERY TECHNOLOGIES.

#### hat, in your opinion, will the cybersecurity landscape look like in 2022? What are the new trends?

Threats will continue to evolve, especially

as attack surfaces continue to grow in this work-from-home scenario spurred on by the pandemic. CISOs will continue to be challenged by this and will need to ensure the provision of consistent and comprehensive security for their employees while they're working remotely and as workloads and applications move to the cloud. I expect this struggle to continue for the next 18-36 months, or as long as the workfrom-home scenario exists. In fact, there is every possibility that the trend might become permanent. From a security practitioner's perspective, I'd say that as the threats keep evolving, the threat detection and response solutions will also need to keep pace, and this is a fact that we'll inevitably have to confront.

From the customer angle, I'd say it's extremely difficult to be a buyer in today's world, mainly because it's easy to get lost in the sea of similar-sounding language and difficult terminologies like EDR, MDR, and XDR, to name a few. Adding to the confusion, customers are now faced with traditional AV and Firewall vendors claiming to be SOC experts – so that in effect, datasheets all look the same. Therefore, it is a priority for us to clearly articulate the value of Secureworks with Taegis as a holistic solution designed to help customers navigate this complex landscape.

#### What organisations in the region need today are battle-tested, best-in-class cybersecurity solutions that reduce risks, improve security operations and accelerate ROI for security and IT teams. How does Secureworks help with this?

One of the biggest challenges that organisations face today is **lack of visibility** – not having line of sight into the entire IT estate. To address this problem, they usually deploy point solution technology for detection purposes which are siloed.

This brings us to the second problem, **complexity**. The technology solutions that organisations deploy, generate a great deal of alert noise at the central monitoring console, making it increasingly difficult to identify the critical incidents that matter most from the sea of alerts – a typical needle in the haystack scenario. Not to mention no alert across silo is correlated.

The third problem is **response**. Assuming that you solve problems one and two, what you get as an outcome is the identified critical incidents that matter. Questions such as, "what can we do about a breach or attack," or "do we have the capability to carry out incident response, and with what resources," become crucial.

Secureworks helps organisations address all these challenges in an effective and seamless manner by helping our customers reduce risk, maximise their existing security and IT investments and fill their security talent gaps. We are recognised as a leader in the industry by

### THERE ARE THREE CLEAR REASONS CIOS AND CISOS LOOK TO US TO SOLVE THEIR FUNDAMENTAL PAIN POINTS. FIRST, TO REDUCE SECURITY IMPACT TO THEIR ORGANISATION, SECOND, TO OPTIMISE THEIR SECURITY INVESTMENTS – NOW AND OVER TIME. AND THIRD, BECAUSE THEY NEED HELP IN NAVIGATING THE SCARCITY OF SECURITY RESOURCES.

global research firms included Gartner, Forrester and Frost & Sullivan. Frost & Sullivan recently named Secureworks its 2021 Company of the Year for Taegis ManagedXDR Innovation.

There are three clear reasons CIOs and CISOs look to us to solve their fundamental pain points. First, to reduce security impact to their organisation, second, to optimise their security investments – now and over time. And third, because they need help in navigating the scarcity of security resources.

Our Taegis software helps solve those pain points because it was purpose-built to be an XDR solution. XDR, at its core, is a big data challenge, and we architected Taegis XDR from day 0 with the XDR vision in mind. The combination of the Taegis platform with analytics and detections, fueled by our deep security expertise gained from engaging in thousands of incident response engagements, monitoring hundreds of threat actor groups from the Secureworks Counter Threat Unit<sup>™</sup>, and insights learned from customers on Taegis XDR, helps protect organisations from today's most pervasive cybersecurity threats.

These constant enhancements to our detection and prevention capabilities by leveraging what we learn about threat actor behavior is a meaningful differentiator for customers. And lastly, our fundamental understanding of how to manage security operations at scale sets us apart. We've been doing this for decades and with the launch of Taegis, we're putting our expertise in the hands of customers and partners.

A comprehensive vulnerability management program is essential for total security. How does Secureworks. with its extensive expertise and worldclass skills, help organisations with this? Vulnerability Management was a serious problem 20 years ago, and it continues to be a serious problem today. Unfortunately, we find ourselves in a situation where the vulnerabilities continue to evolve, but the management of these vulnerabilities remain ineffective because they ignore the actual issue: prioritisation. In my view, the problem with vulnerability management today is not about detection, but about prioritisation in context of one's organisation.

Security teams have been detecting vulnerabilities over the years and passing these to the IT teams to patch, and we have now got to a stage where the IT teams are potentially expected to patch thousands of vulnerabilities every day. By the time they get closer to the target, the next set of vulnerabilities arrive. On top of that, there are severe dependencies on underlying application support, downtimes, etc.

The only way we can solve this problem is by having an effective way to prioritise the vulnerabilities to bring the number to practical numbers instead of thousands.

This is where Secureworks steps in we've been steadfast in our commitment to addressing vulnerabilities and developed Taegis VDR which helps organisations carry out an inventory of their entire assets, detect vulnerabilities, prioritise them and also recommend the remediation of these vulnerabilities. We



prioritise by looking at the likelihood of a vulnerability being exploited times the potential impact on the organisation to determine what should be prioritised in context of the organisation and their overall business. Our solution provides a context to the client about what they should be focusing on, instead of just letting them randomly patch vulnerabilities.

#### What's your plan for the region in 2022? What will your USP be in the highly competitive market, especially in the backdrop of an ever-growing threat/ hacking landscape?

We are expanding to meet increased customer demand. I took on the leadership role in August 2021, and we are building out our sales, marketing and service delivery teams in the region.

This region, in particular, is a fast-

growing market, so we're absolutely committed here.

Additionally, our recent distribution agreement with Redington reinforces our commitment to the channel. The channel is one of our main business drivers in the region and partnering with an organisation like Redington adds advantages for us in various ways. First, their size and scale are helping us take Taegis to a mass market. And second, they have number of born-inthe-cloud partners who are keen to work with Secureworks in the mid-market space.

From a geographic coverage perspective, our focus has been primarily in GCC, and we are now bringing focused attention to the African market with new teams dedicated for South Africa and Emerging Africa.

Therefore, it's not just about 2022 - I'm looking at a plan for the next three years, as far as Secureworks' market presence,

ONE OF THE BIGGEST CHALLENGES THAT ORGANISATIONS FACE TODAY IS LACK OF VISIBILITY – NOT HAVING LINE OF SIGHT INTO THE ENTIRE IT ESTATE. TO ADDRESS THIS PROBLEM, THEY USUALLY DEPLOY POINT SOLUTION TECHNOLOGY FOR DETECTION PURPOSES WHICH ARE SILOED. consolidation and expansion are concerned.

#### What, in your opinion, should an ideal cybersecurity framework look like? What should companies keep in mind while formulating security strategies?

There are many cybersecurity frameworks in the market today that leave organisations spoilt for choice. We advise customers to approach cybersecurity holistically, from four different points: prepare, prevent, detect and respond.

In our region, much attention is given to the prevention side of things. Every technology out there is a "prevention" technology. In my view, there should be equal weightage given to each of these individual points - align your security controls to these 4 areas and see how well you are covered. Also, areas such as continuous threat hunting is extremely important to consider as part of the SOC framework. Design your threat detection framework in such a way that you prevent what you can, detect what you cannot prevent, and hunt what you cannot detect.

The secret to modern-day defence is to approach cybersecurity from every angle and ensure that you increase your security posture and reduce the risk. **1** 

# REASSESSING THE ATTACK-DEFENCE LANDSCAPE

**HARISH CHIB,** VICE-PRESIDENT, MIDDLE EAST & AFRICA AT **SOPHOS,** TELLS **ANITA JOSEPH** ABOUT THE THREAT & SECURITY LANDSCAPE IN 2022, THE EVER-GROWING POPULARITY OF RANSOMWARE AS THE ATTACK OF CHOICE AND THE ROLE THAT AI IS PLAYING IN CYBERSECURITY.



W

cybersecurity landscape looking like, in 2022? What new challenges are

hat is the

we in for?

The speed at which the cyberattack landscape changes, as evidenced in the Sophos 2022 Threat Report, is not going to slow down in 2022. In particular, ransomware attacks on large organizations are increasing, but every organization is a target (even the smaller ones). Having data backed up is not enough of a ransomware defense. Some victims who had their data properly backed up have still chosen to pay large ransoms because they want the stolen data back. Attackers got tired of being thwarted by backups, so they have adopted "multi-extortion" models. We expect this attack methodology to continue.

Sophos also observes an alarmingly common pattern where many security technologies are "working as designed," detecting and preventing stages of attacks, but IT attention on this prevention is oversubscribed leaving business not reacting sufficiently to signals there could be an attack underway (because the products appear to be working). This should be a key area of focus for IT security because adversaries are persistent and will keep trying until they eventually succeed. Layered defenses, with perimeter security, intelligent security and manage detection and response by trained threat hunters are more critical than ever in the coming year. Attackers are smart, persistent and determined. IT security strategies should be as well.

#### Ransomware continues to be the attack of choice for hackers. Where is this headed and what is the impact of Ransomware-as-a-Service?

For many companies, ransomware is one of the biggest cybersecurity concerns. But ransomware attacks are changing all the time. The recently published Sophos 2022 Threat Report highlights the evolution of ransomware as attacks become more service-based and targeted and the attackers turn to additional extortion methods, such as stealing data and threatening to publish or sell it or making aggressive calls to employees, to put pressure on victims to pay.

According to Sophos researchers, over the coming year, a greater proportion of ransomware attacks will be based on ransomware-as-aservice (RaaS) offerings, with specialist ransomware developers focused on creating and then leasing their malicious code and infrastructure to third-party affiliates. Some of the most high-profile ransomware attacks of 2021 involved RaaS, such as the attack on Colonial Pipeline in the US. Ransomware operators can then turn to other cybercriminal services to buy access to hacked victims or use malware delivery platforms to find and target potential victims. These platforms also deliver commodity malware, adware or spam, threats that are less dangerous and disruptive.

What this means for business IT security teams, among other things, is that ransomware attacks are increasingly within range of cybercriminals regardless of their skill levels, as they can just rent or buy what they need; that any infection, for instance, with adware, can lead to every infection, including ransomware, once a target is compromised, so no suspicious signals should be overlooked; and that ransomware attackers will target people as well as technology. Defense-in-depth and human-led threat hunting are two vital protection measures

OVER THE COMING YEAR, A GREATER PROPORTION OF RANSOMWARE ATTACKS WILL BE BASED ON RANSOMWARE-AS-A-SERVICE (RAAS) OFFERINGS, WITH SPECIALIST RANSOMWARE DEVELOPERS FOCUSED ON CREATING AND THEN LEASING THEIR MALICIOUS CODE AND INFRASTRUCTURE TO THIRD-PARTY AFFILIATES. against the rapidly evolving, ruthless threat of ransomware.

## How has the misuse of threat emulation tools impacted cybersecurity?

So-called 'threat emulation' tools such as Cobalt Strike and Metasploit were specifically designed to simulate genuine attacks so that IT security teams can test their defenses under real-world conditions. Unfortunately, these tools have been widely adopted by cyberattackers for malicious intent. The use of such tools is a significant challenge for IT security teams because they provide a ready-made option for less skilled attackers, broadening the field of potential adversaries. They also make it easier for cyber-attackers to deploy and scale their operations and can make it harder for forensic investigators to identify the perpetrators behind an attack. In 2022, Sophos expects cybercriminals to increase their abuse of threat emulation tools. Defenders should check every alert relating to abused legitimate tools or combination of tools, just as they would check a malicious detection, as it could indicate the presence of an intruder in the network.

#### What is the role AI is playing in cybersecurity today? What is it likely to be, going forward?

The application of Artificial Intelligence to cybersecurity will continue and accelerate, as powerful machine learning models prove their worth in threat detection and alert prioritization. At the same time, however, adversaries are expected to make increasing use of AI, progressing over the next few years from AI-enabled disinformation campaigns and spoof social media profiles to watering-hole attack web content, phishing emails and more as advanced deepfake video and voice synthesis technologies become available.

# SPECTRUM NETWORKS, FORTINET PARTNER TO OFFER BEST-IN-CLASS DIGITAL TRANSFORMATION SOLUTIONS

THIS STRATEGIC COLLABORATION WILL HELP REFINE THE DIGITAL SOLUTIONS PORTFOLIO OF COMPANIES AND PROVIDE A SKILLED APPROACH TO TECHNOLOGY ADOPTION.

**"THIS PARTNERSHIP BRINGS TOGETHER THE BEST OF BUSINESS & TECHNOLOGY INSIGHTS, AS WELL AS ASPECTS SUCH AS PRODUCT IDEATION, TECHNOLOGY DEVELOPMENT & DEPLOYMENT AND ORGANIZATIONAL CHANGE MANAGEMENT, TO HELP CLIENTS EXPERIENCE A SEAMLESS AND SECURE DIGITAL TRANSFORMATION PROCESS."** 



pectrum Networks and Fortinet have signed a strategic partnership agreement to combine the best

offerings of both companies-Spectrum Network's industry-leading technology training services and Fortinet's world class cybersecurity solutions. Accordingly, Spectrum will now be an authorized Fortinet Training Center offering Fortinet's industry-defining certification courses in countries such as Saudi Arabia, Pakistan, Bahrain, Oman, Kuwait & Qatar.



Vanessa Sider, Manager, ATC Program at Fortinet

With technology becoming increasingly vital for every aspect of business, companies have recognized the need to accelerate the development of their digital solutions portfolio. This partnership brings together the best of business & technology insights, as well as aspects such as product ideation, technology development & deployment and organizational change management, to help clients experience a seamless and secure digital transformation process.

"The Spectrum Network & Fortinet partnership is a powerful combination," said Vanessa Sider, Manager, ATC Program, at Fortinet. "Fortinet's leadership in the cybersecurity space with that of Spectrum Network's leading technology training services means that organizations in the region will be able to accelerate their cyber security initiatives with top class training – a much needed requirement for fraud prevention across financial, business and government organizations," said Vanessa Sider, Manager, ATC Program, at Fortinet.

""We're glad to join hands with Fortinet, one of the world's leading cyber security vendors as their Authorized Training Center, to provide their certified courses to aforementioned markets," said Pournami Nair, Vice-President-Sales & Alliances, Spectrum Networks.

"Training services have been the core focus for Spectrum right from inception, and over the years we have signed up with best-of-breed technology vendors to be their extended skilling arm in the regions that we represent. This partnership is definitely another notable feather in our cap," she added.

Fortinet, Inc. provides cutting-edge network security solutions and worldclass security appliances, software, and subscription services. Fortinet systems integrate the industry's broadest suite of security technologies including firewall, VPN, antivirus, intrusion prevention (IPS), web filtering, anti-spam, and traffic shaping.

Spectrum Networks is a corporate training and professionals services enterprise serving the Africa, Middle East & Asia Pacific regions. The team has trained over 150,000 professionals by means of a public course schedule and in-house programs – made available through classroom training as well as virtual instructor-led training sessions. The company has been instrumental in skilling up some of the leading business and government entities in the region. Spectrum Networks covers the Middle East as well as the APAC regions, with offices and training centres located in the UAE, KSA, Tunisia, India and Singapore.

To know more, visit the Spectrum Network page that hosts all the Fortinet training courses: https://www.specnt. com/training-service/training-courses/ vendor-specific-courses/fortinet/ 1

# THE ROAD AHEAD

ANITA JOSEPH, EDITOR, SECURITY ADVISOR MIDDLE EAST, SPOKE TO SOME OF THE CYBERSECURITY FRONTRUNNERS TO FIND OUT WHAT THE THREAT-SECURITY LANDSCAPE WILL LOOK LIKE IN 2022.



ow well protected are we today? How ready are we to anticipate attacks and threats? These are two of the most important questions that stare every organization in the face as they enter a

brand-new year, full of uncertainties and probabilities. As the security posture of organizations come under closer scrutiny and hybrid work models become increasingly popular, CIOs are faced with the indomitable task of ensuring that organizations stay protected at all times.

O thing is clear: 2022 will see an increased attack surface and

> "IT'S NO SURPRISE THAT RANSOMWARE IS STILL THE LEADING THREAT TREND. AS THE VALUE OF CRYPTO RISES, THE GREATER THE INCENTIVE FOR CYBERCRIMINALS."

ransomware will continue to be the attack weapon of choice. Artificial Intelligence (AI) will play a greater role in bridging the disconnect between the threat and attack landscape. Organizations will come to rely increasingly on MSSPs and Managed Detection and Response Providers to address their evolving security needs.

According to David Brown, Security Operations Director at Axon Technologies, one of the growing threat trends seen over the last year is targeting Managed Services Providers (MSP) and Cloud Services Providers (CSP). "This targeting allows an attacker to have a significant impact per attack as it can span numerous victims. MSP and CSP have value but also risk. Running on someone's infrastructure means you lost control of how and if that infrastructure is protected," he says.

However, there's little doubt that ransomware is leading the pack. "It's no surprise that ransomware is still the leading threat trend. As the value of crypto rises, the greater the incentive for cybercriminals. Every time a victim pays, it guarantees further attacks against others and, in many cases, repeated attacks upon themselves. In almost all cases of ransomware that we have investigated, unpatched remotely managed or cloud-hosted systems were the initial

#### FEATURE / SECURITY PREDICTIONS



David Brown, Axon Technologies







Rajesh Ganesan, ManageEngine



**"2022 WILL DEMAND A REFOCUSING OF ANTI-RANSOMWARE TACTICS AWAY FROM THE ENCRYPTING MALWARE ITSELF AND ONTO THE INDICATORS OF BEHAVIOR (IOBS) ASSOCIATED WITH RANSOMOPS. ALLOWING THE** DEFENDING ORGANIZATION **TO CIRCUMVENT ENCRYPTION** ENTIRELY."

point of access. These systems loop back to the defence trend of attack surface awareness," Brown adds.

Haider Pasha, Chief Security Officer at Palo Alto Networks, Middle East and Africa (MEA), agrees that ransomware has been on the ascent for much of 2021.

"Through 2021, the EMEA region has seen an increase in cyberattacks, in particular, ransomware attacks have risen in prominence. The Unit 42 Threat Report, 1H 2021 Update found that the average ransom demand increased by 518% and the average ransom paid climbed by 82% from 2020. Part of the evolution is how ransomware functions will continue to evolve, as communities such as nomoreransom.org have fought back, and we are seeing nations lean in further to shut down groups and their campaigns, as well as looking at how they can interrupt or intercept the money flow," he adds.

According to Lior Div, Co-founder & CEO at Cybereason, ransomware has swept the region anew since the pandemic created more complexity in infrastructure and a disconnect between remote-working employees and the IT function.

"For our 2022 predictions, we wanted to go beyond the usual hot topics and

### "WHILE PAST CAMPAIGNS HAVE CONCENTRATED ON THIRD-PARTY STORAGE AND PROCESSING PROVIDERS, 2022 RANSOMOPS RAIDS WILL LEAN TOWARDS DIRECT TARGETING OF THE CUSTOMER SIDE OF THE SHARED-RESPONSIBILITY MODEL."

buzzwords lists that normally pass for insights," said Lior Div, co-founder and CEO, Cybereason. "While it's important for our customers to prepare for more of the same when it comes to things like skills gaps and the use of cloud and AI in cybersecurity, we believe they do not need domain experts to inform them of the obvious. We prefer to focus on the future shape of the threat landscape and what current threat research tells us about risks that may be just over the horizon."

He adds that ransomware has swept the region anew since the pandemic created more complexity in infrastructure and a disconnect between remote-working employees and the IT function. "According to recent Cybereason research, 63% of UAE businesses paid bad actors between US\$350,000 and US\$1.4 million following ransomware incursions in the two years prior to June 2021."

Relatively simple repurposed malware strains have been replaced by RansomOps. Cartels like REvil, Conti, and DarkSide are conducting comprehensive campaigns in which the payload is just the final link in an attack chain. Against this backdrop, 2022 will demand a refocusing of anti-ransomware tactics away from the encrypting malware itself and onto the Indicators of Behavior (IOBs) associated with RansomOps, allowing the defending organization to circumvent encryption entirely.

Rajesh Ganesan, Vice-President at ManageEngine, points out that the cybersecurity skill crunch might force organizations to turn to service providers.

"There is likely to be an imbalance in the supply and demand of skilled employees in the cybersecurity space. To address their evolving needs, organizations will increasingly use the services of MSSPs and managed detection and response providers. For instance, the increase in remote employees, cloud adoption, and the need to meet compliance regulations

> "IF WE WANT TO KEEP ONE THOUGHT IN OUR HEADS FOR 2022, IT IS THAT NOTHING - NO CONSULTANT, NO TOOL, NO PLATFORM, NO PRACTICE, NO POLICY - IS A CATCHALL FOR CYBERATTACKS."

make IAM a tedious process for most organizations. Since many organizations lack the necessary skills and resources to implement an IAM solution, more organizations will turn to Identity as a Service providers to fill this role."

A similar view is endorsed by Willem Hendrickx, SVP International at Vectra AI.

"We have entered an era in which our IT stacks are split across so many environments that internal teams struggle to visualize areas of risk," he says. "In 2022, organizations need to recognize that their change in circumstances demands a rethink of their attack posture. Vectra believes ransomware, which is now increasingly thought of as RansomOps, will now pivot its attention to the exfiltration and encryption of cloud data."

"While past campaigns have concentrated on third-party storage and processing providers, 2022 RansomOps raids will lean towards direct targeting of the customer side of the sharedresponsibility model," he adds.

Vectra also foresees a rise in the demand for managed detection and response (MDR), and especially its capacity to automate key security tasks. The company attributes the upcoming surge to the continuing skills gaps in the regional cybersecurity field, coupled with the increase in complexity of technology environments.

"If we want to keep one thought in our heads for 2022, it is that nothing no consultant, no tool, no platform, no practice, no policy — is a catchall for cyberattacks," Willem urged. "We need to adopt a broader approach and unify human, policy, and technology elements for a more holistic threat posture."

# DEFENDING CYBERSPACE

**DAVID BROWN,** SECURITY OPERATIONS DIRECTOR, **ABED SAMHURI,** CYBER INSTITUTE LEAD AND **ANDREW SCHUMER,** TECHNICAL DIRECTOR AT **AXON TECHNOLOGIES** SPEAK TO ANITA JOSEPH ABOUT EFFECTIVE CYBER DEFENCE, THE IMPORTANCE OF GAMIFICATION IN CYBERSECURITY AND PLANS FOR 2022.



igital Transformation is at an all-time high and continues unabated. What are some of the challenges that hinder its effective implementation?

**DAVID:** To start, I think the biggest hindrance is that most organizations do not understand what digital transformation truly is. They believe it is as simple as deploying the latest "Digital technologies." This belief is not quite true; digital transformation integrates "Digital technology" into every aspect of the organization. This integration radically transforms the organization, which means it undergoes a fundamental cultural shift for employees and its operations.

Due to the lack of understanding of digital transformation, there is often a lack of having the correct strategies in implementing it, which leads to a lack of buy-in from management, employees, customers and inefficient scoping.

## What does effective cyber defence look like?

**DAVID:** In short, effective cyber defence is the design base to allow an organization to maintain confidentiality, integrity, and availability of their business operations. Traditionally, there are 18 accepted standard critical security controls used to outline effective cyber defence strategies. I will not list them all out, but at its core, you have the concepts of cyber hygiene, attack surface awareness, and layered security systems to provide defence in depth wrapped around a resilient framework.

#### Can cybersecurity be enhanced with gamification? How can organizations incorporate gamification into their cyber awareness programs?

**ABED:** Gamification adds emotional engagement to training by providing a competitive context and excitement. Game playing is regarded as a sophisticated way of training and educating security specialists. According to scientific studies, people learn best when they engage their emotions and practical experience in a competitive environment.

Gamification can help in cybersecurity training for both technical and nontechnical people. Cybersecurity professionals will benefit more from games like Capture-the-Flags (CTF) and Cyber Ranges. On the other hand, non-technical people will increase their security awareness by playing fun and engaging games. For example, instead of receiving a lecture on phishing attacks, the audience engages in a game of identifying phishing emails. The game can include scores, leaderboards, trophies, and prizes.

Moreover, games can be individualbased or team-based. In the first type, individuals participate at their own pace and receive scores based on their performance. In the second type, people are grouped into two or more teams that compete between themselves in a game.

Finally, gamified learning has been proven to increase the information

WHETHER YOU ARE MOVING TO THE CLOUD, OPTING FOR SAAS SERVICES OR REBUILDING A DIGITAL CATALOGUE FOR INTERNAL OR EXTERNAL USES, AXON HAS THE TEAM, EXPERTISE AND PEDIGREE TO MAKE THAT TRANSITION SMOOTH AND SUCCESSFUL. retention rate by up to 75%. Because of that, it is an effective approach to sharpen the security awareness of employees, enhance the communication between the team members, and increase the organization's resilience to cyber-attacks.

#### How is Axon Technologies helping companies transform digitally in a secure manner?

**ANDREW:** Axon Technologies is a technology services company that focuses primarily on security and the journey required for a successful outcome in digital transformation. Our methodology is specific to the customer's needs, values, and risks allowing us to deliver a world-class service, ensuring the transformation is sound, focusing specifically on the customer and their expectations. Whether you are moving to the cloud, opting for SaaS services, or rebuilding a digital catalogue for internal or external uses. Axon has the team, expertise, and pedigree to make that transition smooth and successful.

#### What is Axon Technologies planning for 2022, particularly as far as the region's cyber defence and cybersecurity strategies are concerned?

ANDREW: Axon Technologies has a unique offering coming to market in 2022; it will reduce the sprawl and identify the cyber investment in terms of needs and risks. We are also adjusting our market strategy and services around the region's "new paradigm" of working. Our new approach is at the forefront of our strategy. When our customers work from home, abroad, or in an office, we help them tackle the challenges this presents. Our primary goal is to work with IAM vendors and security solution providers to provide a more hands-on and servicebased approach to ensure our customer's successful and secure journey. 🚺

# ARE YOU PREPARED FOR MORE OT THREATS?

or years, Operational Technology (OT) systems have been working to control everything from factories to transportation networks to utilities. The reality is most citizens don't think about these systems until there's a problem. That's why the the attack against Colonial Pipeline in May 2021 was so startling. The attack on a segment of the enterprise transcended IT and resulted in a temporary but severe disruption of the OT based fuel supplies and led the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) to issue an

advisory urging critical infrastructure (CI) asset owners and operators to take on a heightened state of awareness.

Unfortunately, the attack against Colonial Pipeline isn't the first or last time an adversarial cyberattack on an OT target will make headlines. Malicious cyberattacks are likely to increase given the opportunities for mission impact, social anxiety, and profit that disrupting systems and stealing intellectual property from OT and IT systems represent. If there's any silver lining to this high-profile attack it's that it has put a renewed focus on securing critical OT assets.

OT cyber events also have demonstrated the consequence of failing to invest and commit proportionally to a cybersecurity strategy. For years OT system owners relied on the "air gap" that separated OT systems from IT to protect them. But as more and more OT organizations digitally connect OT infrastructure such as supervisory control and data acquisition (SCADA) systems with IT networks, the resulting evaporation of the air gap has dramatically increased the level of risk. Given this situation, it's not a surprise that in the "2021 State of Operational Technology and Cybersecurity Report" 9 out of 10 OT organizations experienced at least

one intrusion in the past year and 63% had three or more intrusions. To protect cyber physical assets, OT organizations need to commit to a proactive cybersecurity strategy, paying particular attention to visibility, control, and behavior analysis. It's critical to protect every point of connection to the outside world to proactively safeguard OT.

#### OT Is No Longer a Niche Exploit

In the past, exploits against SCADA or industrial control systems (ICS) were viewed as an infrequent subset of highly structured and often nationstate sponsored targeted attacks. But the OT market is expected to continue to grow through 2027 at a CAGR of 6.40%. Relying on obscurity as a defense strategy doesn't work anymore; it's practically an invitation to cybercriminals to penetrate and ultimately compromise OT systems. Although IT-related exploits are still more prevalent, according to the Global Threat Landscape Report from FortiGuard Labs, a growing number of exploits are targeting OT. The long-held perception that ICS exploits are an obscure niche of the cyber threat landscape is simply no longer the case.

#### Why Now?

In the past, OT attacks were the domain of specialized threat actors who knew how to exploit ICS and SCADA systems. But now, many of those tools are now being packaged as attack kits on the dark web, so they are available to a much broader set of less technical attackers. The motivations



behind the attacks range from gaining a profit through extortion, stealing intellectual property, to simply testing infrastructure resilience.

#### The Need for Better Visibility

The rapid expansion in the threat landscape and the increase in attacks demonstrate the increased need for integration between enterprise solutions and operational infrastructure. In most cases, security considerations need to extend to on-premise systems and extend to the Internet of Things (IoT) and

> "OT CYBER EVENTS ALSO HAVE DEMONSTRATED THE CONSEQUENCE OF FAILING TO INVEST AND COMMIT PROPORTIONALLY TO A CYBERSECURITY STRATEGY."

Industrial Internet of Things (IIoT) devices. It's also important to have an infrastructure control strategy that restricts and contains suspicious activity and behavior. At a minimum, organizations should implement zerotrust network access (ZTNA), which limits user or device access to only those resources required to perform a specific role or function.

OT organizations that put comprehensive security policies in place give themselves an advantage over threat actors and can limit the impact of a breach. OT infrastructure is no longer benefiting from obscurity and the adoption of near-universal convergence of IT and OT networks implies traditionally isolated environments are no longer safe. Organizations must take proactive steps to harden OT environments, including integrating tools and practices designed to protect, detect, and respond to threats in real-time. Although attacks are inevitable, they don't have to be successful. 1

# CRIMINALISING CYBERCRIME AND RAISING THE RISK FOR CYBER-ATTACKERS

**DAVE RUSSELL,** VP, ENTERPRISE STRATEGY AT VEEAM TELLS SECURITY ADVISOR THAT WHILE IT IS IMPORTANT THAT CYBERCRIME IS PROPERLY 'CRIMINALISED' AND THAT THE PERPETRATORS ARE BROUGHT TO JUSTICE, BUSINESSES MUST UNDERSTAND THE RESPONSIBILITY THEY HAVE TO THEIR CUSTOMERS AND EMPLOYEES TO PROTECT ANY DATA WITHIN THEIR JURISDICTION.

ver the past few years, cyber-attacks have become something which the general public is increasingly aware of.

However, a perception still exists, certainly outside the IT industry, that cyber-attacks are just something that happen on the Internet. It's difficult to relate to and equate the impact of cybercrime on its victims – whether it's an individual who has fallen foul of an online scam or a company that has been forced to pay a ransom to restore its systems. For this reason, it doesn't always seem that cybercrime is viewed or treated like a 'real' crime.

While we acknowledge that cybercrime is an actual crime, for some it might be difficult to get onboard with. The thought of being totally outraged by a hacker taking down a multinational corporation could seem a bit farfetched. This is possibly because of the stereotypes about cybercriminals being painted as disgruntled computer science whizz-kids with nothing better to do than 'stick it to the man.' Consider that the majority of cyber-attacks are the work of huge, organised and wealthy crime syndicates. They are highly sophisticated operations with the aim of stealing money from the business that pays your salary and the government that collects your taxes. Does that sound like a crime?

#### Are we guilty of victim blaming?

The fact is that cybercrime is an actual crime and businesses that fall foul of it are victims. They have suffered a crime committed against them. However, the level of sympathy towards organisations that get breached is very different to what we would give to an individual. If someone tells you they've been hacked, had personal information compromised, and money stolen, your natural reaction probably isn't to say it's their fault. However, cyber breaches are a source of lasting reputational damage to businesses. We tend to assume they did something wrong or acted carelessly. As somebody who has worked in the data protection industry for over 32 years, I would tend to agree with this. The vast majority of cyber incidents are avoidable and the result of organisations failing to follow best practice, poor digital hygiene, and/or outdated or unpatched software.

However, is there any other type of crime that focuses almost exclusively on blaming the victim and so little on bringing the criminals to justice? Businesses are viewed as the guilty party rather than victims and it is accepted that the criminals are unpunishable due to the lack of an agreed global legal framework and justice system.



Dave Russell

If a criminal from another country travels to the USA, for example, and commits a crime against a business on American soil, there is an entire diplomatic process to ensure this person is brought to justice and the victim is compensated. This simply isn't the case when it comes to ransomware.

International and intercontinental co-operation is the only way to create an environment where the risks are higher than the rewards for cyber-attackers. The scourge of ransomware accelerated during the pandemic, increasing the appetite of government and business leaders to break the geopolitical impasse that has enabled cybercriminals to run riot. But it won't be easy, and a workable holistic solution is still years away.

#### Learn self-defence

In the absence of a justice system that completely protects us from the bad guys, basic human survival instinct demands that we learn to defend ourselves. In the context of cybersecurity, that means focusing on a few fundamentals. Firstly, every enterprise needs a dedicated IT security lead in place with access to business leadership and

THE VAST MAJORITY OF CYBER INCIDENTS ARE AVOIDABLE AND THE RESULT OF ORGANISATIONS FAILING TO FOLLOW BEST PRACTICE, POOR DIGITAL HYGIENE, AND/OR OUTDATED OR UNPATCHED SOFTWARE. the authority to lead the security initiative. For smaller businesses, you absolutely need to have a resource with designated responsibility for cybersecurity and specializing in data protection. Secondly, businesses need to practice impeccable digital hygiene. This includes mandatory training for all employees so that they recognise potential attacks, understand who to report them to, and understand why this is important. The more people buy-in to the need for good digital hygiene, the more alert and willing to take the blinkers off they become.

Finally, never ever pay the ransom. Organisations that pay ransoms feed the 'easy pay day' perception that means cybercriminals keep doing it. As soon as businesses stop paying ransoms, we'll see a reduction in the popularity of ransomware as an extortion technique. While businesses who suffer cyber-attacks are indeed victims, they are responsible for protecting any data that they use, process and store. Paying off cybercriminals to get systems back online is an unsustainable defence strategy. As governments become more active in seeking to prevent the spread of ransomware, we may see businesses who do so investigated and reprimanded by independent regulators.

Clearly, dealing with the relentless and mass scale of cybercriminal activity against businesses and individuals will be an international effort across both the public and private sector. While it is important that cybercrime is properly 'criminalised' and that the perpetrators are brought to justice, businesses must understand the responsibility they have to their customers and employees to protect any data within their jurisdiction. This can only be done by implementing a Modern Data Protection strategy that combines effective front-line cybersecurity defences with a comprehensive approach to data backup and disaster recovery. ి

#### FOCUS / THYCOTICCENTRIFY

# THYCOTICCENTRIFY ANNOUNCES ENHANCED CAPABILITIES FOR ITS SECRET SERVER

THE AWARD-WINNING PAM SOLUTION BUILDS ON ITS INDUSTRY-LEADING SECRETS MANAGEMENT CAPABILITIES AND EASE-OF-USE TO OFFER GREATER PROTECTION AND HIGHER PRODUCTIVITY.

Jon Kuhn, Senior Vice-President of Product Management at ThycoticCentrify

> hycoticCentrify, a leading provider of cloud identity security solutions formed by the merger of privileged access management

(PAM) leaders Thycotic and Centrify, has announced new and expanded capabilities for its award-winning PAM solution, Secret Server. With the addition of new security controls, automation, and design updates, Secret Server builds on its industry-leading secrets management capabilities and ease-of-use to offer greater protection and higher productivity.

According to the Verizon 2021 Data Breach Investigations Report, credentials are the primary means by which bad actors hack into an organization, with 61% of breaches attributed to compromised credentials. To reduce this threat, all organizations independent of size, location, or industry need robust, easy-to-use solutions in place to protect the accounts and credentials that allow access to these privileges.

#### Stronger security controls reduce risk

The latest Secret Server release allows

organizations to rotate Secret Server's master encryption key on demand. Rotating individual secrets housed within the digital vault provides an additional layer of protection to block external actors from gaining access to it.

Secret Server also streamlines the connection process for organizations that use jump boxes to protect access to critical resources. Rather than taking time to inject unique credentials at every connection point, users can now use a single key to navigate an entire route from launch, to jump box, to destination within a single session. Users can launch the end-to-end route via Secret Server or the interface of the Connection Manager session management tool.

"Our continued focus on decreasing the steps required to safeguard secrets reduces the workload on security administrators and the attack surface area," said Jon Kuhn, SVP of Product Management at ThycoticCentrify. "As an example, our master encryption key rotation capability is simple to implement and provides an additional layer of protection to block external actors from gaining access to all the other keys stored on the platform."

## Checkout enhancements remove bottlenecks

To enhance auditing and compliance, Secret Server ensures that only one privileged user at a time can use a secret. When secrets aren't checked back in to Secret Server after use, critical maintenance operations can't be performed and productivity slows. The latest release automatically checks in secrets for API connections after expiration.

Additionally, users now have more visibility into remaining time on a secret checkout and can extend the checkout if required.

The latest release also includes enhancements to the Secret Server interface, logging, and reporting to increase usability and accessibility through improved keyboard navigation and screen reader hints.

Organizations can try the latest version of Secret Server for free at https:// thycotic.com/products/secret-server/.

### 10TH EDITION



21 - 23 MARCH 2022 | DUBAI WORLD TRADE CENTRE

# ARAB WORLD'S UNRIVALLED

## **CYBERSECURITY BUSINESS EVENT**

GISEC is the ideal cybersecurity platform to participate & partner with vendors and government entities in the region.

> H.E. Dr. Mohamed Al-Kuwaiti, Head of Cyber Security, United Arab Emirates Government

ENQUIRE ABOUT EXHIBITING, SPEAKING AND SPONSORSHIP 971 (04) 308 6267 | gisec@dwtc.com | #GISEC

OFFICIALLY SUPPORTED BY



OFFICIAL DISTRIBUTION PARTNER



OFFICIAL GOVERNMENT CYBERSECURITY PARTNER







هيئة تنظيم الاتصالات والحكومة الرقمية TELECOMMUNICATIONS AND DIGITAL GOVERNMENT REGULATORY AUTHORITY

STRATEGIC PARTNERS





ORGANISED BY



#### INSIGHT / ESET

# TOP 10 CYBERSECURITY HABITS TO SHED IN 2022

BE ALERT, BE PROACTIVE AND BREAK THESE BAD HABITS TO IMPROVE YOUR CYBER-HYGIENE IN 2022 *Phil Muncaster, guest writer at ESET* 

he new year is a new opportunity to rewire your digital life. An increasingly important part of this is cybersecurity. In fact, 2021 is

already shaping up to have been one of the most prolific years yet for cybercriminals. Almost 19 billion records were exposed in the first half of the year alone.

Better security should mean you're more insulated from the risk of identity fraud and financial loss. The cost of these scams reached a record \$56bn in 2020, with most of this coming online. Although the organizations you interact with have a duty, and often a legal responsibility, to keep your data protected, it's important to do your bit.

If you're still feeling reluctant to find new ways to protect your digital world, consider this: a third of US identity crime victims have claimed they didn't have enough money to buy food or pay for utilities last year as a result of fraud, according to the U.S. Identity Theft Resource Center. Be alert, be proactive and break these 10 bad habits to improve your cyber-hygiene in 2022:

#### Using outdated software

Vulnerabilities in operating systems, browsers and other software on your PCs and devices are one of the top ways cybercriminals can attack. The problem is that more of these bugs were discovered in 2020 than any year previously: over 18,100. That amounts to more than 50 new software vulnerabilities per day. The good news is that by switching on automatic update functionality and clicking through to update when prompted, this task needn't intrude too much on day-to-day life.

#### Poor password hygiene

Passwords represent the keys to our digital front door. Unfortunately, as we have so many to remember these days – around 100 on average – we tend to use them insecurely. Using the same password for multiple accounts and easy-to-guess credentials gives hackers a massive advantage. They have software to crack weak encryption, try commonly used variants and attempt to use breached passwords across other accounts (known as credential stuffing). Instead, use a password manager to remember and recall strong, unique passwords or passphrases. And switch on two-factor authentication (2FA) on any account that offers it.

#### Using public Wi-Fi

We're all getting out-and-about more these days. And that brings with it a temptation to use public-Wi-Fi. But there are risks. Hackers can use the same networks to eavesdrop on your internet usage, access your accounts and steal your identity. To stay safe, try to avoid these public hotspots altogether. If you must use them, don't log-in to any important accounts while connected.



#### Not thinking before clicking

Phishing is one of the most prolific cyberthreats out there. It uses a technique known as social engineering, where the attacker tries to trick their victim into clicking on a malicious link or opening a malware-laden attachment. They take advantage of our hard-wired credulity, and often try to force rapid decision-making by lending the message a sense of urgency. The number one rule to thwart these attacks is to think before you click. Double check with the person or company sending the email to make sure it is legitimate. Take a breath. Don't be pressured into taking over-hasty action.

#### Not using security on all devices

It goes without saying that in an era of prolific cyber-threats, you should have anti-malware protection from a reputable provider on all of your PCs and laptops. But how many of us extend the same security to our mobile and tablet devices? Research suggests we spend nearly 5,000 hours each year using these gadgets. And there's plenty of opportunity to come across malicious apps and websites in that time. Protect your device today.

#### Using non-secure websites

HTTPS sites use encryption to protect the traffic going from your web browser to the site in question. It has two purposes: to authenticate that website as genuine and not a phishing or fraudulent web property; and to ensure cybercriminals can't eavesdrop on your communications to steal passwords and financial information. It's not a 100% guarantee nothing bad will happen as even many phishing sites use HTTPS these days. But it's a good start. Always look for the padlock symbol.

#### Sharing work and personal lives

Many of us have spent a large part of the past two years merging a once clearly defined line between our work and our personal lives. As the line has become more blurred, cyber-risk has crept in. Consider the use of work emails and passwords to register on consumer shopping and other sites. What if those sites are breached? Now hackers may be able to hijack your corporate account. Using unprotected personal devices for work also adds extra risk. Keeping business and pleasure discrete is worth the extra effort.

A THIRD OF US IDENTITY CRIME VICTIMS HAVE CLAIMED THEY DIDN'T HAVE ENOUGH MONEY TO BUY FOOD OR PAY FOR UTILITIES LAST YEAR AS A RESULT OF FRAUD, ACCORDING TO THE US IDENTITY THEFT RESOURCE CENTER.

#### Giving out details over the phone

Just as email and SMS-based phishing uses social engineering techniques to trick users into clicking, so voice phishing, also called vishing, is an increasingly popular way to elicit personal and financial info from victims. The scammers often disguise their real number to add legitimacy to the attack. The best rule of thumb is not to hand out any sensitive info over the phone. Ask who they are and where they're calling from and then ring the company direct to check – not using any phone numbers provided by the caller.

#### Not backing up

Ransomware is costing businesses hundreds of millions annually. So it's sometimes easy to forget that there are still variants lying in wait for consumers. Imagine if you were suddenly locked out of your home PC. All the data on it, and potentially cloud storage, could be lost forever – including family photos and important work documents. Regular backups, according to the 3-2-1 best practice rule, provide peace-of-mind in case the worst happens.

#### Not protecting the smart home

Nearly a third of European houses are fitted out with smart gadgets like voice assistants, smart TVs, and security cameras. But by fitting them with connectivity and intelligence, these devices also become a more attractive target for criminals. They can be hijacked and turned into botnets to launch attacks on others, or used as a gateway to the rest of your devices and data. To keep them secure, change default passwords on start-up. Also, be sure to choose a vendor who has a track record of fixing known vulnerabilities in their products and research potential security flaws before purchasing a gadget.

We're all looking forward to what 2022 has in store. Make sure it's a year full of only good surprises by improving your personal cybersecurity today.

# TACKLING CYBERTHREAT THE INTELLIGENT WAY

**WERNO GEVERS,** REGIONAL MANAGER AT MIMECAST MIDDLE EAST, TELLS ANITA JOSEPH THAT IN ADDITION TO PROVIDING OUTSTANDING EMAIL PROTECTION, MIMECAST ALSO PARTNERS WITH THE WORLD'S BEST SECURITY VENDORS TO BUILD AN INDUSTRY-LEADING CYBER RESILIENCE ECOSYSTEM, WHICH NOW HAS MORE THAN 100 API PARTNERS.





hat is the cyberthreat and security landscape looking like in 2022?

Armed with sophisticated and

brute-force attack methods, threat actors continue to capitalise on the ongoing disruption of the pandemic and are leveraging the world's shift to digital services to launch cyberattacks at an unprecedented scale. In 2022 cybercrime will continue to disrupt our increasingly digital workplaces and lifestyles.

The growing importance of business productivity suites, email and cloud communication services will continue to provide attackers with optimal channels to target their victims, demanding new strategies and tools from organisations and their security teams.

The last two years have seen an acceleration in companies' digital transformation efforts as they enabled hybrid work and explored new channels for reaching and serving customers. However, the mass move to remote work has exposed security vulnerabilities many companies didn't even know existed. Cybercriminals have also capitalised on employees' psychological vulnerabilities through increasingly sophisticated and opportunistic social engineering campaigns. Cybersecurity awareness training will need to shift from an event to a culture embedded deep within the business.

Ransomware will also continue to wreak havoc following a successful 2021 for criminals. The rise of Ransomware-as-a-Service is potentially arming more threat actors than ever before with dangerous cyberattack tools that could cause untold disruption and economic damage. Lives could also be at risk. The emergence of 'killware', which involves attacks using ransomware or other malware to target critical systems, is worrying. Since attackers deploying killware are solely intent on causing harm and even death, the potential damage they can cause is immeasurable.

## What is the importance of targeted threat protection in today's threat ecosystem?

Email is an organisation's most important communication platform, and the application that is most susceptible to attack. Organisations and their employees are targets for increasingly sophisticated and targeted attacks designed to steal money, credentials, customer data, and other valuable intellectual property. Targeted threat protection defends against attackers trying to steal data or credentials, plant ransomware, trick employees into transferring money, and springboard to attack supply chains. These kinds of threats require advanced security measures over and above those provided by traditional email security systems. That's because traditional email security can't combat cybercriminals' advanced threats.

#### Tell us more about Mimecast Email Security- What are some of its key features and why should customers opt for it in 2022?

Email remains the No. 1 initial attack vector,

and the volume of email-based threats (phishing, impersonation and other targeted email attacks) has only increased since the start of the COVID-19 pandemic. Mimecast Email Security empowers customers to protect their businesses from whatever volume and variety of email-based threats come their way. It is a multi-layered email security solution that provides:

• Advanced security – Secure email gateway defends against email-borne impersonation attempts, malicious URLs at time-of-click, known and unknown malware, spam, internal threats, malicious and accidental information loss.

• Threat protection, threat intelligence and threat remediation – Detects attacks at and inside the email perimeter, providing deep threat intelligence and the ability to contain cybersecurity threats.

• **Business continuity** – Ensures email availability in the event of an outage of a primary email system.

• Brand exploit protection – Protects against both the abuse of domains owned by a brand and imitation using domains not owned by the organisation, in part by leveraging DMARC.

• Browser isolation – Allows users to safely click on any embedded URL and surf the web.

• Internal email protect – Extends Mimecast's security controls to an organisation's internally generated emails.

> EMAIL REMAINS THE NO. 1 INITIAL ATTACK VECTOR, AND THE VOLUME OF EMAIL-BASED THREATS (PHISHING, IMPERSONATION AND OTHER TARGETED EMAIL ATTACKS) HAS ONLY INCREASED SINCE THE START OF THE COVID-19 PANDEMIC.

#### • Security awareness training -

Reduces employee security mistakes with relevant training and tactical security tests.

In addition to outstanding email protection, Mimecast also partners with the world's best security vendors to build an industry-leading cyber resilience ecosystem, which now has more than 100 API partners. Each integration is designed to allow organisations to gain greater insights into their threat landscape, reducing complexity, minimising risk, and improving threat detection and response times.

#### How does Mimecast's threat intelligence help organizations better understand the threats that they face?

As email-borne attacks continue to evolve, threat intelligence is key to identifying and mitigating sophisticated attacks that do serious damage to an organisation.

Threat intelligence is data and knowledge about known and emerging security threats, including what they look like, how they work, how they impact an organisation and how they can be stopped. Threat intelligence is particularly important for identifying and blocking new threats – having access to upto-the-minute data on information gleaned from email threats worldwide is critical to stopping a mail attack before it can breach defenses and wreak havoc.

Mimecast Threat Intelligence is designed to give a deeper understanding of the cyberthreats organisations face and provide Mimecast's expert analysis of the attacks detected. The service provides threat data and analytics specific to each organisation. The threat intelligence is developed by the Mimecast Security Operations Center (MSOC). The team of globally distributed analysts and security researchers continuously monitors threats across billions of emails each month, analysing and investigating attacks to develop sophisticated and timely threat intelligence and to rapidly apply updates to Mimecast security solutions. 1

# THE 6 TECHNOLOGY TRENDS AFFECTING THE SECURITY SECTOR IN 2022

**ETTIENE VAN DER WATT,** REGIONAL DIRECTOR – MIDDLE EAST & AFRICA AT AXIS COMMUNICATIONS

Ettiene van der Watt

he beginning month of any year is characterised by many articles listing the technology trends that will shape industry sectors in

the next one. But over the years, one can see a pattern develop, a roadmap that reveals the sentiments, and technologies we should be prioritising.

In this case, the keyword is 'trust', which is an interesting one. The 2021 Edelman Trust Barometer shows that among online survey respondents in 28 countries, trust in the technology sector is declining globally, along with concerns of climate change, job losses, and cyberattacks. Worries that are all valid to the global security and surveillance sector.

In the pursuit of realising a smarter, safer, and more sustainable world built on the back of a trustworthy and reliable ecosystem of innovation, these are the technologies and insights that will continue to transform security in 2022 and beyond.

#### A post-pandemic world

The impact of the COVID-19 pandemic continues to be felt in multiple ways. We see its physical manifestation in the challenges to supply chains, with global manufacturing brought to a near standstill and companies having to re-evaluate where and how they source key components and equipment for their respective products and services. We also see it in deployed technology – how intelligent solutions in video and monitoring are used to enforce social distancing and implement public health strategies.

A global shortage of semiconductors has also seen companies explore in-house manufacturing and the potential of system on a chip (SoC) for relevant sectors. While this may be a very specific trend, combined with the substantial shifts caused by the pandemic, more businesses will consider SoCs for their security solutions going forward.

#### Embracing a sustainable future

Sustainability is no longer just a trend, nor should it be deemed as such. With a global focus and push towards environmentally friendly principles and practices, exemplified by initiatives such as the UN Sustainable Development Goals towards industry, human settlements, and consumption and production, a business must exhibit sustainability in its offerings and examine new possibilities through a sustainable lens.

Companies must pay closer attention to their processes from end to end. They need to scrutinise their products and services in terms of sustainability factors, such as power efficiency, building materials, and ethical deployments. These discussions are already taking place at events like Expo 2020, where the conversations have taken on a more forward-thinking position, and real progress is being made for long-term impact. More conversations like this need to be had, and it's up to companies to facilitate them.

## Healthy scepticism equals effective cybersecurity

We don't always think of scepticism as a positive trait, but in relation to cybersecurity it can be a prudent one. In a highly connected world with an increasing number of interconnected systems, comprehensive security strategies must ensure that if one area is compromised, the rest of the system won't collapse.

A trend that's emerged from taking a sceptical eve towards technology is zero trust networks. Built on the fundamental assumption that no device or entity connected to a network can be trusted, the deployment of these architectural setups is likely to accelerate and become the default approach. In turn, this will dramatically impact video surveillance in the form of encryption, identification, and hardware and software maintenance. COVID-19 has also played a role in forming this approach, as remote working solutions call for more connected devices in a wider context.

This high-impact technology conference at Expo 2020 further unpacks cybersecurity as the cornerstone of trust.

#### 5G is connecting the world

What is commonly used as a buzzword for the next era of internet connectivity is starting to see realworld applications. With 5G networks projected to cover one-third of the world's population by 2025, this technology is starting to make its way into the security and network video surveillance sectors, hinting at it being more than just a trend.

A specific 5G-related trend that is likely to grow in leaps and bounds is the deployment of private 5G networks – wireless networks that use 5G-enabled technology and dedicated bandwidth to serve as a closed solution for a company. They are faster than public networks, more reliable, and offer an ideal situation for specific industries. These networks also present security benefits which, when applied to the sector, could potentially streamline and improve solutions of varying size. This specific manifestation of technology is one to watch out for.

#### Artificial intelligence, formalised

No trends piece for the next decade would be complete without mentioning artificial intelligence (AI). In the case of security and surveillance, this ranges from image quality and analytics to

COMPANIES MUST PAY CLOSER ATTENTION TO THEIR PROCESSES FROM END-TO-END. THEY NEED TO SCRUTINISE THEIR PRODUCTS AND SERVICES IN TERMS OF SUSTAINABILITY FACTORS, SUCH AS POWER EFFICIENCY, BUILDING MATERIALS AND ETHICAL DEPLOYMENTS. camera configuration and performance. By taking a simple process and applying AI to it, you optimise that process to its full potential.

With more widespread use comes the need for regulation, specifically for the applications of AI. The solution is legislation on multiple levels of governance, ensuring AI is being used ethically and without bias. With a common agreement on local, regional, and international levels, we will be able to lay the foundation for the next industrial revolution and the growth of other technological trends, most notably smart cities.

#### Increased authentication measures

With the question of trust and increased scrutiny in cybersecurity, authenticity is becoming the next big hurdle in the age of data manipulation. This is valid for both hardware networks and video surveillance itself. How can you trust surveillance when you assign no value to its authenticity?

Deepfake technology is a growing threat. With improved methods of manipulating and altering images and videos, the authenticity of captured real-world events and people is compromised. This is not a problem exclusive to the security sector, but it is one that requires comprehensive solutions to overcome, such as applying digital signatures and verifying the source of data to specific hardware. The application of AI also shows promise in being able to detect when manipulation has occurred. Regardless, this is a challenge that multiple sectors have to contend with and work harder to combat.

All these trends factor into the need for businesses and other entities to rethink their security solutions for 2022 and beyond. With a focused and driven approach and by embracing the technology of the future, today's challenges can be met head-on.

# MEASURING AND MITIGATING AND MITIGATING CYBER RISK SAKET MODI, CEO & CO-FOUNDER AT SAFE SECURITY

s businesses continue to invest in digital transformation and base their business models on technology, cyber threats

only become more imminent. Cyber Risk is no longer an IT problem, but a board-room concern. With cyberattacks disrupting business continuity, they pose a direct impact on the top and bottom line of an organization's balance sheet. Thus, making cybersecurity one of the top priorities of every organization.

## Challenges with traditional cybersecurity approach

The evolving breach trends verify that complying to frameworks alone can no longer holistically safeguard organizations. Frameworks such as ISO, NIST, PCI DSS and others are used as reference checklists for cybersecurity and risk management practices, however, they provide limited visibility. Cybersecurity must be aligned in every organization; threats and mission-critical business needs, provided by products that deliver holistic and actionable insights. The Frameworks approach to riskposture assessments is subjective, laborintensive, and only offers point-in-time snapshots/assessments. They rely on a qualitative scale without any objective and quantitative measure to assess the security posture of an organization.

Similarly, Security Rating Services represent an independent source of publicly accessible data to support some use cases. However, these services don't provide a complete assessment of security controls, as their information is primarily sourced from publicly accessing internet IP addresses, honeypots, analyzing Deep and Dark web content, and individual proprietary data warehouses.

#### New approach to cybersecurity

Today, the delegation of risk decisions to the IT team cannot be the only solution and has to be a shared responsibility. The board and business executives are expected to incorporate the management of cyber risk as part of their business strategy since they are accountable to stakeholders, regulators and customers. For the CROs, CISOs, and Security and Risk Management Professionals to be on the same page, there has to be a single source of truth for communicating the impact that cyber risk has on business outcomes, in a language that everyone can understand.

This is where Cyber Risk Quantification



becomes a game-changer. There is a need for a solution which integrates with the entire security stack and gives a measurable analysis that supplements decision making. This comprehensive information empowers CISOs and executives to make informed and timely data backed decisions to ensure the cybersecurity of the organization.

Continuous Assessment of Cyber Security is the need of the hour Compliance and government guidelines mandate the move to go beyond periodic assessments and into continuous monitoring of sensitive and critical information. In such situations, a CISO may often be unable to quantify the maturity of the Information Security measures deployed in the organization. Continuous Assessment of cybersecurity risk posture lets an organization prioritize the key focus areas across their Critical Assets and most vulnerable technology, third parties or employees. This ensures that adequate measures towards holistic

### CYBERSECURITY MUST BE ALIGNED IN EVERY ORGANIZATION; THREATS AND MISSION-CRITICAL BUSINESS NEEDS, PROVIDED BY PRODUCTS THAT DELIVER HOLISTIC AND ACTIONABLE INSIGHTS.

Cyber Security maturity are adopted throughout the organization.

## Objectivity and simplicity should be at the core of a cybersecurity strategy

Cybersecurity posture cannot be represented by lengthy reports anymore. It needs to become objective and help decision makers across the organization truly understand the risk posture and the financial value of risk that the organization faces. It also needs to be free from IT jargons to enable the boardroom to have a clearer view of the risk posture, thereby facilitating data driven and informed decisions. Executives can get overwhelmed with excruciating details from multiple tools or people. They can now rely on all the data that has been collected and converted from these sources into a simple yet comprehensive risk metric that they can use to track and build their trust on.

#### Benefits of Cyber Risk Quantification

With quantified cybersecurity risk management practices, organizations have:

• A unified cybersecurity strategy: Cybersecurity that is presently siloed, will have a single pane of glass view for security leaders to make guicker, data-

driven decisions.

• An objective metric of communication: The potential financial impact of a cyber attack converts its risks to a direct business threat. It becomes a simple and effective means to communicate risks to all internal and external stakeholders.

**Real-time visibility:** Dynamic visibility of what is going well and what needs improvement is enabled by a real-time cohesive output - breach-likelihood across people, process, technology, and third-party.

# kaspersky PERSONAL EMPLOYEE INFORMATION LEAKAGE IS THE LEAST DISCLOSED TYPE OF BREACH IN THE UAE

KASPERSKY'S GLOBAL SURVEY OF IT BUSINESS DECISION-MAKERS PROVIDES INSIGHTS INTO HOW WELL ORGANIZATIONS AND WORKERS COLLABORATE AND PROTECT THEMSELVES, THEIR CLIENTS AND EACH OTHER.

he Kaspersky Employee Wellbeing 2021 report unveils that while organizations regularly face employee data leakage, almost third of companies in the UAE (30%) prefer not to disclose these incidents publicly. At the same time, staff may lack basic cybersecurity knowledge to protect themselves as only 39% of businesses offer IT security training.

A successful corporate cyber-defence is impossible without employees at all levels joining forces. Technology is important to prevent cyberattacks but human factors still play a crucial role, being tied to 85% of incidents. Kaspersky's global survey of IT business decision-makers provides insights into how well organizations and workers collaborate and protect themselves, their clients and each other.

Despite high-profile cases of data breaches being mainly associated with stealing customer information, personal employee data is very popular with cybercriminals as well. In 2021, more than a third (42%) of organizations weren't able to provide complete security of their workers' data and faced incidents involving this type of information.

The fact that 30% of affected organizations haven't disclosed a breach of personal employee data publicly is a sign that the problem is bigger than it seems. As for the rest, 65% have shared information about an incident proactively and 6% did so after it has been leaked to the media. This shows that this type of leak is the least frequently disclosed, compared to corporate or customer data breaches.

According to the research, only 39% of organizations have already implemented security education and training to ensure that employees are provided with crucial information. In addition, more than two thirds (84%) of those companies have experienced at least one issue relating to the quality of these services. This includes dissatisfaction with the high complexity of courses and a lack of support or expertise on the part of the training provider.

In 2021, compliance of staff and dealing with insufficient end-user security culture is one of the top three biggest concerns for businesses when it comes to IT security – 32% of respondents cited it among the most alarming issues. In practice, companies regularly face informational security infringements (45%), inappropriate

THE FACT THAT 30% OF AFFECTED ORGANIZATIONS HAVEN'T DISCLOSED A BREACH OF PERSONAL EMPLOYEE DATA PUBLICLY IS A SIGN THAT THE PROBLEM IS BIGGER THAN IT SEEMS. IT resource use (52%), and improper sharing of data via mobile devices (51%).

Breach prevention requires concerted action by everyone who interacts with a corporate system and could be a potential target for attackers. To better secure employees, companies should combine reliable protective measures with maintaining security awareness among their teams. This includes:

• Ensuring prompt patching and updating of software to prevent adversaries penetrating the system.

• Implementing high-grade encryption for sensitive data and enforcing strong credentials and multi-factor authentication.

• Using effective endpoint protection with threat detection and response capabilities to block access attempts, and managed protection services for efficient attack investigation and expert response.

• Minimizing the number of people with access to crucial data. Breaches are more likely to occur in organizations where too many employees work with confidential and valuable information that can be sold or somehow used.

• Equipping your employees with the cybersecurity skills they need. Provide education that presents all the necessary and up-to-date information in an engaging format. To save time and receive a quality service, companies should work with globally recognized providers that can ensure an efficient learning process.

# CONTINUOUS PEN TESTING FOR ACTIVE DIRECTORY



### Is Your Active Directory Prepared for a Ransomware Attack?

Active Directory is the prime target for ransomware attackers. However, it is woefully unprotected. Attivo Networks disrupts these attacks with unprecedented visibility to exposures, vulnerabilities, and live attacks.

Over 200 Active Directory security checks show risks and detect attacks that lead to domain control for downloading malware, changing security settings, and establishing backdoors. Over 75% of assessments show multiple high-risk exposures. Are you ready? Get a free health check to see.



attivonetworks.com







Storage

Recording

AI Detection

**Stunning Colors and Detail** 

2K Resolution

ULTRA 2K resolution and the F2.0 aperture work in tandem to produce vivid images that give you the complete picture.



Vision

Audio

Spotlight

Secure in Extreme Weather Conditions

With an IP67 weatherproof-rating, Outdoor Cam Pro boasts greater protection against the elements than any of its competitors.



ind Alexa

#### Subscription Free Security

Installation

Equipped with a 32GB memory card and on-device AI, Outdoor Cam Pro offers security that is ready out of the box. \*The device can support up to 128G.



Notifies You Only When Needed

The camera's built-in AI accurately identifies when a person is present. This means that you are only notified when an event occurs that requires your attention.



Color Detail at Night

The built-in spotlight illuminates the surrounding area when motion is detected and allows the camera to capture footage in vivid color. Giving you a much clearer view of who's there.



**Flexible Installation** 

The Magnetic Mount and 20ft Cable allow you to easily install the camera anywhere on your property.

# AED 299/-

### CUL Innovations

### Available at all leading electronics stores.