ISSUE 68 | SEPTEMBER 2022

WWW.TAHAWULTECH.COM

ADVISOR

MIDDLE EAST

HIGHLIGHTS

Sec

MICRO FOCUS (PG 8) GBM (PG 18) TENABLE (PG 20)

THE POWER OF THREATINTELIGENCE

AMIR KANAAN, MANAGING DIRECTOR FOR THE MIDDLE EAST, TURKEY AND AFRICA AT KASPERSKY TALKS ABOUT WHY THREAT INTELLIGENCE IS ESSENTIAL FOR GOVERNMENT AND ORGANISATIONS TO STAY ONE STEP AHEAD OF TARGETED ATTACKS.



NUCLIAS CLOUD BUSINESS GATEWAY

POWERFUL and ENDURING

multi-aspect protection for SMB cloud networks



DBG-2000

Why You Want It





Zero Touch Provisioning Cloud-Based Management



Intrusion Prevention System



Dynamic Web

Content Filtering



Application Control

Auto VPN Ap



☑ info.me@me.dlink.com

https://me.dlink.com

CONTENTS









2 THE POWER OF THREAT INTELLIGENCE

News roundup from the security industry in the region and beyond.

6

8

Toufic Derbass, MEA Managing Director at Micro Focus, on how the company's cutting-edge SMAX platform leverages AI to provide the best experience to customers as they adapt to a digitally transforming business ecosystem.



36 Ajay Nawani, Director -Sales Engineering, MEA at Sophos, on ransomware, MDR & Threat Intelligence.



Make the most of WiFi 6.

Linksys Atlas Pro 6 with Intelligent Mesh[™] is a dual-band WiFi 6 system that delivers next-level streaming, data traffic and uninterrupted video conferencing to more than 30 devices per node simultaneously.

Access to 160 MHz — the least congested channels available on the 5GHz band — unleashes WiFi 6's incredibly fast connectivity.



Dual-band Mesh WiFi 6 system

Up to 3,5X faster speeds than WiFi 5[°].

Mesh WiFi 6 delivers true gigabit speeds—up to 5.4 Gbps with 6-stream connectivity—throughout your entire home or business, inside & out.

160 MHz capable.

Access to the least congested channels on the 5 GHz band unleashes the true power of WiFi 6, allowing work-from-home, online learning, streaming & gaming devices to operate simultaneously without reduced bandwidth.

More WiFi Channels.

Dynamic Frequency Selection (DFS) provides access to more channels, reducing interference from neighbouring networks.

Industry-leading technology.

The Qualcomm" Immersive Home 216 Platform transforms home & business NiFi to wired-like stability & speed.

Easy setup & control.

t's simple to set up and lets you manage your network or prioritise devices from anywhere, all with the free Linksys app. **30+ devices** Capacity per node. 맘

AX5400 Accumulated speed up to 5.4 Gbps.



Covers homes with up to

2-3 bedrooms per node (±230 m²/1 floor).



Model# MX5500 Available in 1-, 2- or 3-Pack: MX5501, MX5502, MX5503

Linksys.com

*As compared from 802.11ac to 802.11ax.



EDITOR'S NOTE



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

> Anita Joseph Editor

EVENTS



THREAT INTELLIGENCE REDEFINED

SPOTLIGHT THREAT

INTELLIGENCE

Threat Intelligence or Cyber Threat

Intelligence, is data that is collected, processed, and analysed to understand a threat actor's motives, targets, and attack behaviours. As it turns out, key components such as cyber threat intelligence can strategically guide security practices, align organisational objectives and ensure the success of those objectives. Cyber Threat Intelligence also provides increased visibility across the threat landscape into existing threats and

emerging cyber-attacks. By acquiring this knowledge and applying

it to the environment, one can reduce the risk of data loss, prevent or minimise disruption to business operations, and increase one's understanding of the threat to help prevent future attacks.

In this issue, we highlight the power of Threat Intelligence brought to you by the expert himself: Amir Kanaan, Managing Director for the Middle East, Turkey and Africa at Kaspersky. In a detailed conversation for our cover story, he explains why Threat Intelligence is essential for government and organisations to stay one step ahead of cybercriminals.

From Intelligence we move to Trust. In an exclusive interview, Hani Nofal, Vice President of Digital Infrastructure Solutions at GBM, talks about enterprise security and what organisations must do to build public trust. Meanwhile, Ajay Nawani, Director -Sales Engineering, MEA at Sophos gets into the finer details of ransomware, MDR and Threat Intelligenceall vital for building a robust security framework.

That's not all: Marcus Josefsson, Vice President Sales, Nozomi Networks,

> unravels the nuances of IoT security and how the company is constantly focused on helping regional organisations

with critical IoT networks build a solid cybersecurity framework.

If you thought it ends there, it doesn't. We have a special feature on International Women In Cybersecurity Day, where the powerful women voices in the security industry make their presence felt. We also have an exclusive opinion piece from Maher Jadallah, Senior Director Middle East & North Africa at Tenable, who tells us all about botnets and how they can be dealt with effectively. In addition to this, we have the usual news and insight columns offering you a pan-industry perspective of the security industry and where it's headed. Happy Reading!

Published by

FOUNDER, CPI Dominic De Sousa (1959-2015)

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

OnlineEditor

Daniel Shepherd

daniel.shepherd@cpimediagroup.com

PRODUCTION AND DESIGN Designer Prajith Payyapilly prajith.payyapilly@cpimediagroup.com DIGITAL SERVICES Web Developer Adarsh Snehajan webmaster@cpimediagroup.com Publication licensed by Dubai Production City, DCCA PO Box 13700 Dubai, UAE

Tel: +971 4 5682993

© Copyright 2022 CPI All rights reserved

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

Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com

Sales Director Sabita Miranda sabita.miranda@cpimediagroup.com

MALWARE STEALING CREDENTIALS & CREDIT CARD DETAILS TARGETS GAMERS IN ME



from untrustworthy

resources for free, players got malicious software instead, losing their gaming accounts and even funds. These and other findings are part of the gaming-related threats report issued by Kaspersky.

To assess the current landscape in gaming risks, Kaspersky experts observed the most popular PC and mobile games-related threats. Globally over the year (from 1 July, 2021 to 30 June, 2022), Kaspersky security solutions detected more than 384,000 users affected by almost 92,000 malicious or unwanted unique files that mimicked 28 games or series of games.

Over the same period, in the Middle East 6,290 unique users were affected by 5,135 malicious and unwanted files. Egypt and in Saudi Arabia had the highest numbers of users affected (2,768 and 2,324 respectively).

"During the pandemic the gaming industry was greatly boosted, increasing the number of gaming fans several times over. As we can see, cybercriminals are actively abusing this trend, creating more and more new schemes and tools to attack players and steal their credit card data and even game accounts, which can contain expensive skins that can later be sold. We expect to see new types of attacks on gamers in the next year. For example, strikes on e-sports, which are now gaining huge popularity around the world. That's why it's so important to always be protected, so you don't lose your money, credentials, and gaming account," said Anton V. Ivanov, senior security researcher at Kaspersky.

ARUBA TO SHOWCASE SECURE EDGE-TO-CLOUD NETWORKING SOLUTIONS AT GITEX TECHNOLOGY WEEK 2022

In October this year, Aruba, a Hewlett

Packard Enterprise company, will return to GITEX Technology Week, exhibiting under the theme 'Making connections, anywhere' - creating the connections that power businesses and the world.

In its 13th appearance at the event, the company will demonstrate its cloud-native approach to helping customers meet their connectivity, security, and financial requirements across campus, branch, data center, and remote worker environments, covering all aspects of wired, wireless LAN, and wide area networking (WAN).

Commenting on the company's participation at GITEX, Jacob Chacko, Regional Director - Middle East, Saudi & South Africa at Aruba said, "At Aruba, we believe the most dynamic customer



experiences happen at

the Edge - an office, a hospital, a school, and at home.

It's anyplace work gets done and data is generated by users, devices, and things across your network. Our mission is to help customers capitalise on these opportunities by providing secure edgeto-cloud networking solutions. We use Albased machine learning to deliver simpler, faster, and more automated networks that analyse data to help businesses thrive."

CYBERARROW & G42 CLOUD ANNOUNCE PARTNERSHIP TO ENHANCE CYBERSECURITY IN PUBLIC AND PRIVATE ENTITIES

Innovative cyber security provider,

CyberArrow, has signed a new Memorandum of Understanding with pioneering AI and Cloud Computing organisation G42 Cloud to host and support delivery of their services.

G42 Cloud is a subsidiary of leading AI and cloud computing provider G42, and its powerful cloud and market presence will help CyberArrow to continue to scale its operations and reach public and private entities across MENA by becoming one of the ecosystem partners that can be hosted and deployed to customers on G42 Cloud.

CyberArrow works with organisations of all sizes, supporting them to enhance their cyber security resilience and posture. By acquiring the CyberArrow GRC solution, businesses of all sizes can now save thousands of hours on cyber security GRC tasks while ensuring full



compliance with international- and local standards.

The new agreement will allow for the automation of a wide array of Governance, Risk Management, and Compliance (GRC) tasks, helping both the government and those working within private entities to become more secure. Amar Basic, Co-Founder of CyberArrow, said, "We are excited to be working with G42 Cloud. Their work is well recognised in the region, and this new MoU will help us to strengthen our offering within the MENA region as well as allowing us to offer our solutions to an even larger audience.

EMT DISTRIBUTION ANNOUNCES PARTNERSHIP WITH DAST VULNERABILITY SCANNER VENDOR CRASHTEST SECURITY FOR ME & AFRICA

PARTNERSHIP ANNOUNCEMENT -----

emt

CRASHTEST

SECURITY

emt Distribution, a major IT & IT Security product distributor based on

Security product distributor based on security, IT Management, and analytic solutions, has announced an enhanced partnership with Crashtest Security DAST vulnerability scanner helping you automate your security scanning and achieve protection at DevOps speed

Crashtest Security is a SaaS-based security vulnerability scanner allowing agile development teams to ensure continuous security before every release.

"Application Security has always been critical and considered to be difficult to manage- We bust that myth by introducing Crashtest Security, a fully automated application pen-testing tool which keeps the organisation safe from threats by continues scanning. We are excited to announce our strategic global alliance with Crashtest security to help our customer across the Middle East and Africa via our robust channel fraternity." said Mir Hamid Ali – BU Head, emt Distribution

"We are thrilled to partner with emt Technology Distribution and introduce Crashtest Security's automated pen testing tool to the region and make continuous security a go to approach to agile development." commented Felix Brombacher, Co-founder & Managing Director-Crashtest Security.

VEEAM PROMOTES MOHAMAD RIZK TO REGIONAL HEAD FOR MIDDLE EAST AND CIS

Veeam Software, the leader in backup, recovery and data management solutions that deliver Modern Data



Protection, has announced the appointment of Mohamad Rizk as Regional Director for the Middle East and CIS region. In this new role, which plays to his strengths as a leader with a strong business acumen, Rizk will support Veeam's continued investment and strong presence in the region and will look to grow the company's market share and revenues through the planning and execution of sales and channel strategies.

Rizk has had an illustrious career helping regional enterprises with their digital transformation journeys through the rollout of technologies, primarily relating to virtualisation, storage, and data management and protection. He joined Veeam as a Presales Consultant in 2013 and moved up to his last role of Senior Director, Technical Sales – Middle East, Russia & CIS where he was instrumental in the planning and execution of several projects that helped drive Veeam's reputation as an industry leader in Modern Data Protection,

KIM ANSTETT APPOINTED TRELLIX CHIEF INFORMATION OFFICER

Trellix, the cybersecurity company

delivering the future of extended detection and response (XDR), has announced Kim Anstett has joined Trellix as Chief Information Officer (CIO). As CIO, Anstett leads Trellix's global information and technology systems organisation and joins the Executive Leadership Team (ELT).

"Kim has a proven record of building highperforming IT organisations," said Bryan Palma, CEO of Trellix. "No doubt she will do the same at Trellix while also serving as our "customer zero" for our market leading products."

Trellix is focused on accelerating the use of XDR architecture across enterprises, commercial businesses and governments to both advance organisation security posture and to ease cybersecurity incident response and management. As CIO, Anstett is responsible for executing a technology strategy designed to drive efficiency, flexibility and innovation across the business. "My number one priority as Chief Information Officer at Trellix is to deliver insights



to our business to serve our customers. Second is furthering diversity, equity, inclusion and development for my teams," said Anstett, CIO of Trellix. "I am motivated by people, process and technology; and I see a lot of alignment with Trellix's ethos as a home for soulful work."

PUTTING THE CUSTOMER FIRST

TOUFIC DERBASS, MEA MANAGING DIRECTOR AT MICRO FOCUS, ON HOW THE COMPANY'S CUTTING-EDGE SERVICE MANAGEMENT AUTOMATION X (SMAX) PLATFORM LEVERAGES AI TO PROVIDE THE BEST EXPERIENCE TO CUSTOMERS AS THEY ADAPT TO A DIGITALLY TRANSFORMING BUSINESS ECOSYSTEM.

hat is Micro Focus's approach towards Enterprise Service Management (ESM) and the evolution of

the service desk?

Today, companies of all sizes are focusing on innovation by not only adopting new technologies, but also by rethinking how they've traditionally approached delivery of goods and services to their customers and employees. Therefore, it isn't surprising that one of the top priorities of CIOs, based on multiple surveys, is to "delight" the customer and employees, that consume IT services. On the same list of CIOs priorities, we can also always find service management across the entire enterprise. CIOs must improve, support and deliver services in ways that transform their business. So, we speak here not about a commoditised service desk but about transformational service management, and this is what Enterprise Service Management is about.

In this context- three main trends in service management that can help CIOs

succeed at their objectives are:

- Focusing on enterprise services, just not IT services.
- Delivering better, more immersive IT experiences to delight everyone.
- Utilising AI & automation to improve service delivery and experiences.

These are the three guiding principles for us at Micro Focus when designing our service management platform and the content.

What are the essential capabilities that are mandatory in an ESM platform?

A modern and effective ESM platform must be equipped with modular content. For example, our platform is SMAX, which stands for Service Management Automation X. It comes with content including applications for ITSM (implementing the best practices from ITIL v4), non-IT service management like HR support request management, IT asset management, and hybrid OUR CUSTOMERS REPORT THAT THEY WERE ABLE TO EXPAND THE INFLUENCE OF ENTERPRISE FOOTPRINT WITH MICRO FOCUS SMAX BECAUSE OF ITS ENTIRELY CODELESS PLATFORM.

cloud management. The platform has an embedded foundation consisting of discovery, CMDB and automation and orchestration software.

An ESM platform should deliver the following values:

 Superior service experience by powering self-service with AI, extending service desk reach to become an enterprise-wide service





desk, and intelligent collaboration.

- Optimised IT productivity by configuring without code, fulfilling requests faster with the help of AI, and automating anything, including cloud service provisioning.
- Cost control and raised resiliency by removing unpredictable costs, driving successful changes, and governing IT assets
- Deployment flexibility: on-premise, cloud and SaaS, to be aligned to the customer cloud strategy.

You want to help your employees get back to work faster, and here AI-based capabilities help, such as search, ticket creation and conversational virtual agents. Then again, you'd want to transform your service management into a fast and flexible operation through codeless workflows, enterprise-wide automation, and fulfilling requests faster with AI. But there's more. You should be able to connect your service management workflows with powerful orchestration. From our single platform, you can provision hybrid cloud services. Even difficult to automate manual processes can be handled by RPA robots that mimic screen-based human actions.

How are Micro Focus customers leveraging and benefiting from Micro Focus SMAX?

We have customers ranging from Small, Medium and Enterprises level, using our services. What's common for all of them is the time to value by adopting our codeless way of working, the embedded Al-powered automation, superior user experience, and the deployment flexibility from on-premises, cloud, or SaaS, to we help them improve their maturity and be aligned to their cloud strategy.

Without exception, our customers report that they were able to increase

THE PLATFORM HAS AN EMBEDDED FOUNDATION CONSISTING OF DISCOVERY, CMDB AND AUTOMATION AND ORCHESTRATION SOFTWARE. the usage of the service desk and the self-service portal. At the same time, the volume of tickets decreased. Our customers also report that they were able to expand the influence of enterprise footprint with Micro Focus SMAX because of its entirely codeless platform. Many customers developed codeless applications for different use cases and automated processes in HR, payroll, facilities and other business units. This helped digitise the "back offices".

Our SaaS customers appreciate the fact that they are always up-to-date with the latest release and that with the basic license they get 50 license units of Universal Discovery and two Operations Orchestration (00) workflows. The simple and transparent licensing without any hidden costs is also something all of our customers love about Micro Focus SMAX. They get the most of enterprise service management capabilities with basic SMAX licence, such as all ITSM workflows, native CMDB and studio for configuring codeless workflows, HR service management content with 35 HRspecific workflows, mobile application for employees and field support engineers. 1









Believe the hype, it's here. ENTER THE NEXT DIGITAL UNIVERSE

#GITEXGLOBAL gitex.com 170+ COUNTRIES

ERICSSON

700+ STARTUPS **4000+** companies



GOLD SPONSORS

PLATINUM & LANYARD SPONSOR



ATTENDEES BADGE SPONSOR

VINFAS



MAJLIS LOUNGE SPONSOR ManageEngine

SILVER SPONSOR

------ INNOVATION PARTNER ------









THE POWER OF THREAT INTELLIGENCE

AMIR KANAAN, MANAGING DIRECTOR FOR THE MIDDLE EAST, TURKEY AND AFRICA AT KASPERSKY TALKS ABOUT WHY THREAT INTELLIGENCE IS ESSENTIAL FOR GOVERNMENT AND ORGANISATIONS TO STAY ONE STEP AHEAD OF TARGETED ATTACKS.

ell us about Kaspersky's operations in the Middle East?

We have had our operations in the Middle East for over 15 years and are celebrating our 25th anniversary this year. Earlier this year, we

opened a new office in Saudi Arabia, which adds to our ever-expanding network and is a milestone in our roadmap to protect over 400 million users and 240,000 corporate clients worldwide. With quarter of a century experience, we continue to work closely with major government entities and key industries in the region doing what we do best – protect our customer and what they value the most. To date, we have tracked activities of over 900 APT groups and collected over 1 billion malware files.

To illustrate our success in numbers, we have had steady growth in our Middle East business throughout the past years. The first half of 2022 showed a 8% YoY growth and we aim to continue this streak of success in the region.

Digital transformation raises the stakes for IT security. This basically means moving your IT security strategy to a new level. How does Kaspersky's Threat Intelligence step in to help organisations stay ahead of cyberthreats?

APT groups are extremely smart, well-equipped to infiltrate any device or network to achieve their motives. They are also quick to exploit vulnerabilities in new technologies. For example, IoT has fast become a key driver of digital transformation and is crucial within today's smart city infrastructure. The Mirai botnet used enterprise-class IoT devices to launch massive DDoS attack that had dire financial and reputation consequences. APT groups also rely on smart social engineering techniques to infiltrate their victims. The only way to stay ahead of the threats is by understanding them and preparing accordingly. For example, an airline company in the Middle East using our threat Intelligence can have access to insights on APTs targeting other airlines in the region and worldwide to understand the criminals' motives and techniques and build a cybersecurity strategy that is resilient.

Our research team is an elite group of more than 40 security experts, specialised in tracking and studying the activity of APT groups around the world. Our regional researchers are currently

ALTHOUGH THE CYBERSECURITY INDUSTRY IS CREATING MORE SECURITY → TECHNOLOGIES, IT IS OFTEN MERELY PLAYING CATCH-UP WITH THE ATTACKERS. monitoring 29 groups in the Middle East and have issued hundreds of reports sharing expertise and insights on their operations.

Kaspersky has created a concept for designing IT systems with "innate" immunity, called the Cyber Immune approach. How do you implement this and ensure that IT systems are innately secure?

Whether it is industrial plants, energy facilities, cars or smart city systems, critical infrastructure cannot afford to have operations disrupted as this could affect people's lives . Although the cybersecurity industry is creating more security technologies, it is often merely playing catch-up with the attackers. So, Kaspersky decided to reinvent cybersecurity and coin the term "Cyber Immunity", a way to develop IT systems with innate protection. Kaspersky's Cyber Immune approach is a means to create solutions that are virtually impossible to compromise and that minimise the number of potential vulnerabilities. Think of it as cybersecurity at the core, rather than being required to add additional layers of protection at a later stage.

We believe that Cyber Immunity is the future of cybersecurity. Our Cyber Immune operating system, KasperskyOS, along with a special development methodology, lets developers create Cyber Immune solutions. It provides the interfaces, mechanisms and tools, while the methodology requires organisations to clearly define security objectives and the conditions in which a IT system will operate.

We've already launched products based on our Kaspersky OS. We recently launched the Kaspersky IoT Secure Gateway 1000, which is a Cyber Immune solution. Kaspersky IoT Secure Gateway 1000 is designed to serve as a secure gateway for the Internet of Things in an enterprise network.

Traditional approaches to security are no longer enough. Today, a holistic TO ILLUSTRATE OUR SUCCESS IN NUMBERS, WE HAVE HAD STEADY GROWTH IN OUR MIDDLE EAST BUSINESS THROUGHOUT THE PAST YEARS.

approach is necessary to stay ahead of the fast-growing threat landscape. How much of this is actually implemented in businesses in the region? What are they lacking?

Organisations are investing in a holistic



cybersecurity approach. However, we are seeing a shortage of holistic cybersecurity approaches backed by strong expertise, which in the long run will always be a liability.

As compared to other global

economies, our region is no exception to the dearth of talent in cybersecurity, more so in critical infrastructure industries like energy, transport, oil & gas and so on. 66% of organisations have faced significant security staffing

challenges. We want to reduce this percentage, if not make it irrelevant. To do so, we work closely with various government entities and universities to train, teach and hone new and existing talent. To combat lack of security skills, we also offer our Managed Detection and Response to organisations. Through this, organisations can get access to our experts round the clock, and can expect individually tailored ongoing detection, prioritisation, investigation and swift response to incidents.

Awareness is the first step to effective cybersecurity. How much awareness is there among organisations in the region about the growing importance of fool-proof security practices? Also, how do you view the training and capacity building capabilities available in the region?

We at Kaspersky absolutely agree that

OUR RESEARCH TEAM IS AN ELITE GROUP OF MORE THAN 40 SECURITY EXPERTS, SPECIALISED IN TRACKING AND STUDYING THE ACTIVITY OF APT GROUPS AROUND THE WORLD.



awareness is the first step to effective cybersecurity. But, organisations fail to understand that awareness is not a "one-off" thing, but an ongoing process. Majority of all cyber-incidents are caused by human error because it takes only one click on the wrong link to let cybercriminals inside an organisation. A cybersafe workplace culture implemented at all levels in an organisation, from the boardroom to the workforce has the potential to defend against attacks.

We understand that people are generally not motivated to change their habits, and sometimes educational efforts turn into an empty formality. This is why using our insights, expertise and training techniques, we have designed a continuous learning approach that can help the staff play their part in the overall cyber safety of the organisation. Our Kaspersky Automated Security Awareness Platform (ASAP) takes a new approach to online educational programs. It doesn't just provide knowledge: it builds concrete cyber-hygiene skills and practices.

In order to fight modern global cyberthreats, it's not enough to just build a Security Operations Center (SOC) in the conventional sense – you need a SOC that is equipped with the technologies, security intelligence and knowledge that empower it to adapt to ongoing challenges. How does Kaspersky power SOCs to fight complex and complicated threats?

SOC building is a complex, costly, and long-term project. It may fail due to various reasons, given the demand for it to be intelligence-driven and have the ability to provide round-the-clock monitoring and response.

> WE BELIEVE THAT CYBER IMMUNITY IS THE FUTURE OF CYBERSECURITY.

TO COMBAT LACK OF SECURITY SKILLS, WE ALSO OFFER OUR MANAGED DETECTION AND RESPONSE TO ORGANISATIONS.

Our approach is based on handson experience in SOC building and operating, commercial threat hunting, APT campaigns investigations and analysing more than 380,000 new threats every day. For the SOC framework, we help organisations choose the right technologies that fit well with their business needs by understanding their processes, the nature of their business and the industry they operate in. We then move towards identifying the data most crucial for them and their customers, and ensure it's protected.

Our SOC consulting service includes the following stages:

1. Data Collection and Review: At this stage, Kaspersky assesses the existing detection and response capabilities of the SOC team, collects data needed for the framework development, and reviews the existing documents related to security operations.

2. Design: The Kaspersky team will develop complete and consistent SOC framework tailored to the customer infrastructure, requirements and needs.

3. Build: Kaspersky can also help organisations upgrade their existing SOC from traditional to next-gen or if the situation calls for it, build one from scratch to mitigate emerging threats.

4. Implementation: The Kaspersky team in coordination with the SOC team will deploy and configure Kaspersky tools and solutions needed for SOC operation. Deployment and configuration of third-party solutions can be provided by partners or customers, if needed.



5. Talent recruitment: It is very important that the SOC team has all necessary roles, right skills and follow well-defined processes and procedures. Kaspersky helps organisations by interviewing candidates applying for IT/ security positions to fit the bill.

6. Support: After the SOC starts its operation, the Kaspersky team will support its daily operation throughout the agreed time period. Kaspersky experts will support security operations in various ways, such as:

a. Using the Kaspersky Managed Detection and Response services for the most sophisticated tasks, such as incident response, digital forensics, malware analysis and security assessment

b. Consultation regarding previously designed SOC processes and procedures

c. Technical support for Kaspersky solutions

OUR KASPERSKY AUTOMATED SECURITY AWARENESS PLATFORM TAKES A NEW APPROACH TO ONLINE EDUCATIONAL PROGRAMS.

d. Red teaming exercises and maturity assessment for continuous SOC improvement

When I started my career in the IT industry more than 15 years ago, a SOC was a cybersecurity luxury and often only needed within governments. Fast forward to today, where SOCs are a main pillar of cybersecurity and play a vital role in keep an organisation one step ahead of emerging threats.



BUILDING TRUST

HANI NOFAL, VP OF DIGITAL INFRASTRUCTURE SOLUTIONS AT GBM, TELLS ANITA JOSEPH ABOUT ENTERPRISE SECURITY AND WHAT ORGANISATIONS MUST DO TO BUILD PUBLIC TRUST.

hile cybersecurity can play a major role in organisations' digital transformation strategies, many admit that they are underprepared, or view risk management programs as a low priority. How have the nature of security challenges evolved in recent months?

The increased use of technology has created a rich playground for cyber criminals to take advantage of. With the move to hybrid working environments, as well as rapid digital transformation, the threat landscape has expanded, and cyber criminals have become even more sophisticated, affecting businesses on several fronts. Cyber security has long been challenged to keep pace with the threat landscape, but it struggles to gain significant support from business leaders, often not until it's too late. More recently though, cybersecurity maturity is appearing in business RFPs, and with a highly connected digital supply chain, the expectation is that organisations will not become threat vectors to business partners.

Investing in cybersecurity now is not just about securing your organisation, but making sure you're not a risk to business partners. Vetting third parties is becoming more common, as there have been alarming cases of cyberattacks, like the more recent examples of supply chain hacks such as SolarWinds and Kaseya that were delivered via the software vendors own update systems.

Ransomware has also become more prevalent, with attacks on the rise both globally and regionally. According to IBM's 2022 Threat Force Intelligence Index, ransomware and server access attacks were the top attack types observed in the Middle East and Africa, tying for first place each representing 18% of attacks. Ransomware was also the dominant attack type observed across cyber incidents in the UAE.

There has also been a re-prioritising of risks for CIOs in the aftermath postpandemic. According to the most recent GBM Security Report, Data Security, Cloud Security and Secure Remote Access and Connectivity, are top of mind when Gulf organisations choose to invest in security.

Are there common pitfalls that you see organisations facing today when building their cybersecurity strategies?

There are various pitfalls organisations can fall into when building their security strategies. Some of the more common examples we see are organisations not incorporating automation into their strategies. As time goes by, repetitive tasks that are appropriate for automation pile up and can sometimes bog down IT teams. Machine learning and automation can help free up IT teams to focus on more demanding tasks. Considering security as just a function of IT is another drawback. Security presents many of today's biggest organisational challenges and is entwined into every aspect of the business. Organisations need to take a holistic approach to mitigating security risk, by focusing on people, processes, technology and business priorities.

Another important pitfall is organisations thinking they are immune to cyberthreats. Many businesses believe that they will not be hit by a cyberattack until it actually happens. With cyber threats, it's not a matter of if, but when they will happen. The right security strategy looks to predict, prevent, detect and respond to every kind of risk.

Based on GBM's recent report on 'digital trust', what steps should organisations be taking to build public trust?

Enterprises have an important role to play in the goal of engendering mutual online trust that benefits all of society, whilst reducing the opportunities for threat actors to negatively impact any of us. To build public trust, enterprises need to embrace three constituents: Customers, Employees, and Business Partners.

The customer relationship is often more keenly focused upon, and clearly adhering to customer expectations towards data privacy and online security is more critical than simply complying with legislation – customers expect more than this.

Employees, who are the front line in any customer engagement, need to feel safe and secure in their working environments, which must translate into secure devices, identities, systems and a simple way to ensure this remains so. Arduous security processes will create friction at an employee level which can leak into customer interactions.

Business partners are becoming more digitally connected, and so ensuring an enterprise's integrity within the industry supply chain is becoming a requirement these days.

All these areas demand a robust risk management capability: understanding the risks to the enterprise and its connected ecosystem, understanding not all risks are the same, and applying the appropriate level of control for the identified risks.

Are there essential policies or systems that organisations in the region need to take into consideration to increase their resiliency in a rapidly changing environment?

Cybercrime, like other crimes, may never be eradicated, but we should be able to reduce the impact and burden to enterprises and individuals if we work together more effectively.

Government regulators should mandate the sharing of breach data – since we learn more from others mistakes then their best practices. Enterprises must also realize they are fighting a war against experts and need expertise to help - it cannot be won alone. Additionally, technology and service providers need to work with both groups, as technical advisors, to help identify how best to implement, apply and comply with regulations.

GBM has recently expanded its capabilities in managed security services. What motivated that investment, and what do you hope to bring to market in the near term? GBM believes that, unless the technology you are investing in delivers clear core

INVESTING IN CYBERSECURITY NOW IS NOT JUST ABOUT SECURING YOUR ORGANISATION, BUT MAKING SURE YOU'RE NOT A RISK TO BUSINESS PARTNERS.

competitive differentiation, it should be outsourced, and this is the role of Managed Security Service Providers. As organisations outsource more of their own security processes to professional partners, they can refocus security investment and resources into areas that add more value, such as hiring individuals to monitor for ongoing breaches. This will support customers to further grow, innovate, and address the security challenges faced due to rapid evolution in technology.

We've recently announced the acquisition of the majority shares of Coordinates Middle East, a regional Managed Detection & Response firm. With this move, we're enhancing our suite of cybersecurity offerings to include Cor., Coordinates' innovative technology-agnostic platform, that enables integration, automation, and orchestration across detection, response, and remediation of any technology to achieve cyber resilience.

The innovation engine, platform, and disruptive approach to cyber defense will help organisations to address challenges faced with legacy Managed Security Services that are historically complex to deploy, challenging to adopt, slow to respond to events, and resource-heavy on enterprises. Through this acquisition, we will bring to market state-of-the-art technology further boosting its ability to anticipate, detect and respond to cyber threats, helping to support enterprises of all sizes to defend against emerging cybersecurity threats. **1**

GBM BELIEVES THAT, UNLESS THE TECHNOLOGY YOU → ARE INVESTING IN DELIVERS CLEAR CORE COMPETITIVE DIFFERENTIATION, IT SHOULD BE OUTSOURCED.

MEETING ENEMYBOT HEAD-ON

MAHER JADALLAH, SENIOR DIRECTOR MIDDLE EAST & NORTH AFRICA AT TENABLE, TELLS US ABOUT BOTNETS AND HOW THEY CAN BE DEALT WITH .



otnets first gained widespread notoriety in the early 2000s and continue to be a common and disruptive source of trouble

around the globe. Since the start of the COVID-19 pandemic, cybercriminals have stepped up their attacks against individuals and institutions alike, spurred on by increasing digitalisation, according to the Global Cybersecurity Outlook 2022 published by the World Economic Forum [1].

Proof of this unfortunate trend reared its head in May this year, when research by AT&T Alien Labs found that EnemyBot operators were exploiting recently identified vulnerabilities across content management system servers, Android and other IoT devices [2]. What this means in plain English is that the gap between a vulnerability being discovered and it being exploited is shrinking.

EnemyBot was first discovered in March 2022 and is actually the sum of code taken from other disruptive botnets including Mirai, Qbot and Zbot. Some experts describe it as an updated version of Gafgyt_tor, as it leverages a number of botnet functions sourced from the Gafgyt codebase. What makes Enemybot a bigger concern is that its code can be easily found online, which makes it a do-it-yourself botnet for nefarious individuals to bend to their needs.

Trouble Compounded

In today's digital world, securing devices and networks has become challenging due to several issues. Coming back to EnemyBot, threat actors are actively developing this botnet, meaning the criticality of a vulnerability can change from one moment to the next.

Since this botnet is modified regularly to take advantage of new vulnerabilities, it is difficult to protect against; each time threat actors hear of a vulnerability and realise they stand to benefit from exploiting it, it's a given that they will rapidly tweak the botnet to achieve their goals. In some cases, vulnerabilities don't even have CVE numbers by the time they are exploited by EnemyBot or other such attacks.

Another unfortunate issue complicating the security landscape is that it is now easier to launch a cyberattack today than in years gone by. The result of this is cybercrime has become a thriving business across the globe with a supporting ecosystem [3].

Ultimately, the majority of cyberattacks come down to vulnerabilities that are left unchecked. Each day vulnerabilities are discovered and security advisories are issued, however this deluge of information makes it challenging for professionals

ANOTHER UNFORTUNATE ISSUE COMPLICATING THE SECURITY LANDSCAPE IS THAT IT IS NOW EASIER TO LAUNCH A CYBERATTACK TODAY THAN IN THE YEARS GONE BY.

to discern a real threat from one that is theoretical – an unlocked car with valuables inside only becomes a real threat if cybercriminals realise there are valuables sitting inside the unlocked car.

Effective Security Basics

While the threat landscape is more potent than ever before, organisations can take simple but effective steps to protect themselves, starting with minimising their attack surface area.

Organisations must kick this process off by maintaining up-to-date asset inventory that showcases everything they have, so vulnerabilities relating to specific assets can be addressed before they are exploited. This time consuming process is the cornerstone of any fully-fledged security program, as it can provide an organisation with critical insights that they can act on.

An up-to-date inventory of assets means an organisation must identify all assets (known and previously unknown)



in its environment, which includes software and firmware versions, each asset's patch levels and communication/ connectivity paths. While network monitoring will provide a reasonable level of detail here, it is critical organisations perform active and device/systemspecific querying to paint an accurate picture of an asset and its vulnerabilities.

Once an organisation's asset inventory is up-to-date, the focus should be to perform vulnerability assessments regularly, so vulnerabilities can be addressed before they can be exploited. It cannot be emphasised enough that it's vital to stay up-to-date on the latest threats, especially those that impact frequently targeted solutions such as Microsoft, VMware and F5.

Threat actors are acutely aware that the easiest way to take advantage of an organisation's assets is to go after points of entry they are unaware of. This agility, as demonstrated by EnemyBot, means that organisations must become even more vigilant with their defenses. An organisation that makes the effort to fully catalogue its technology stack and supplements this with frequent threat assessments is far more secure than one that lacks these insights and preparedness. As threat actors step up their game, the onus is on organisations to respond with equal or greater vigor.

Links:

[1] World Economic Forum - Global Cybersecurity Outlook 2022

[2] Rapidly evolving IoT malware EnemyBot now targeting Content Management System servers and Android devices

[3] Tenable – A look inside the ransomware ecosystem 1

<section-header>

nternational Women in Cyber Day (IWCD) began as an occasion to provide support and recognition for women in cybersecurity. Today, the movement, celebrated on September 1 every year, is inspiring women from around the world to create and host events to celebrate their role in cybersecurity. We asked some of the well-known faces in the industry what it means to be a woman in the dynamic and highly competitive cybersecurity arena. Here's what they said: Andrea Carter- Senior Director, Marketing, North, South and Emerging EMEA, Sophos, has been working for the last ten years in cybersecurity at Sophos, and according to her, she "couldn't ask for a more interesting and rewarding role." In her opinion, cybersecurity and the cyber threat landscape are all changing rapidly, and this is a steep, lifelong learning curve, "but you will constantly have an interesting and varied career which is extremely motivating. The best part of being a woman in the



cybersecurity industry is having the opportunity to work in such a high paced, exciting environment where no day is the same and you can guarantee you will be doing something new continuously."

So, what made her choose this field?

"I was lucky enough to almost fall into IT, gaining my first role within a sales automation software company. I very quickly realised that I had a passion for technology and have spent my entire working career of nearly 20 years since YOU GET TO GAIN SOME OF THE MOST SOUGHT-AFTER SKILLS AND WORK WITH SOME OF THE SMARTEST PEOPLE EVER. in the B2B technology sector. I think the reason I have remained in the technology sector and love it so much is the constant rate of innovation which keeps my role interesting and exciting," she says.

Then again, what are the ups and downs of taking up this career?

Andrea believes that the greatest challenge, "for a leadership role like mine, is to align the team's goal to the goal of your organisation. At times it is difficult to maintain this alignment



ROYA GORDON, SECURITY RESEARCH EVANGELIST AT NOZOMI NETWORKS



HEATHER MAHALIK, FELLOW INSTRUCTOR AT SANS INSTITUTE



DEEPA KUPPUSWAMY, DIRECTOR OF SECURITY AT MANAGEENGINE

in all the circumstances. I make sure that there is transparency in my team and every person on my team should be clear on the role they are playing to enable Sophos to reach its goals. This helps to maintain the positive energy of the team. Constant communication and 360-degree feedback helps to align the team with the organisation."

Ciara Campbell, Security Engineer at Tenable says there's no 'typical'

career in cybersecurity. "That's what makes the sector so exciting," she savs. "Security can be about prevention and detection but I wouldn't say it just comes down to those two aspects. Each person's job in this sector can be vastly different from another person in the same industry. There are many layers to security which is what makes it such a fun industry to work in. You are always learning something new no matter how long you have been in the industry. It's a really friendly and supportive industry to have a career. People working in cybersecurity are always willing to help others and share their knowledge."

In her opinion, a career in cyber means we're constantly looking at what's possible, whether it's right or wrong, good or bad, successful

BEING IN THE THICK OF A SECURITY INCIDENT AND DRIVING THE INCIDENT RESPONSE PROCESS SUCCESSFULLY BRINGS AN ADRENALINE RUSH EVERY TIME.

THE REASON I'VE REMAINED IN THE TECHNOLOGY SECTOR AND LOVE IT SO MUCH IS THE CONSTANT RATE OF INNOVATION WHICH KEEPS MY ROLE INTERESTING AND EXCITING.

or a dead end. Threat actors are constantly finding new attack paths and we're working to find them first to shut them off.

Ciara says she came into her career in cybersecurity/technology later in life than most. "Having worked in retail banking for a number of years, I made the decision to go back to University as a mature student. As soon as I began my degree, I loved it and knew this was the right career path for me. I've not looked back and so far it's been great fun and I have worked with some of the best people. I learn something new every day, not necessarily always something technical which is fantastic. If you want to work in an exciting and fast changing environment with huge opportunities for growth then Security is the industry to be in. I can't honestly think of any other industry I would rather work in," she adds.

Deepa Kuppuswamy, Director of Security at ManageEngine transitioned from product engineering to the information

security domain 10 years ago. "It was a new domain and I wanted to explore and master it," she says. "The role required me to align with business objectives, make the different teams understand the value of security and privacy, while at the same time acting as a business enabler helping the organisation grow in a secure way. I was intrigued enough to choose this career path since it posed a different challenge."

Deepa chose this field because "no

two days are the same working in the security domain. I love the challenge of building a security and data protection program to fit into our organisation's culture, and to engineer and scale our security tools and processes as the business evolves and scales up. Being in the thick of a security incident and driving the incident response process successfully brings an adrenaline rush every time. It's also fulfilling to brainstorm with various business units to understand their unique problems and come up with solutions to improve the security posture. The fact that my work contributes to the greater mission of securing the organisation and its stakeholders is what motivates me."

According to Deepa, the upside about a career in security is that one is a life-long learner once you choose this career. "It never gets boring and dull. There is always the need to be up-to-date on security threats and new technologies, there is always something new to learn and tryout. The fast-paced environment makes this career interesting and fulfilling. One more positive fact is the high demand for qualified cybersecurity professionals. Organisations in nearly every industry have openings in the cybersecurity field.

IN CYBERSECURITY, EVERY DAY IS DIFFERENT, AND TECHNOLOGY CONSTANTLY CHANGES.

While ManageEngine understands the importance of cybersecurity, on the other side, some young professionals may feel stuck or helpless when the management doesn't really understand the importance of cybersecurity for businesses. An organisation culture which does not prioritise, values and respects cybersecurity might be demotivating. In such cases, the constant need to keep advocating for your cause can dampen your spirit and lead to burnout."

Heather Mahalik, Fellow Instructor at SANS Institute loves the fact that in her

job, every day is different, and technology constantly changes. "As a hobby, I enjoy doing puzzles. DIFR is the ultimate puzzle. The way I see it is that my job is not work, it's fun. I love what I do and I love working with the people I have on my teams.

In fact, Heather says, cybersecurity chose her and not the other way round. "Seriously, it did. I was in the right place at the right time and an opportunity came my way. I thought it would be a stepping stone into another profession, but it was love at first byte."

For Roya Gordon, Security Research Evangelist at Nozomi Networks, being

in cybersecurity is one of the most exciting and fulfilling careers she's had. "You can choose your own adventure. If you like forensics and investigation, sales, or media, you can do it in cybersecurity."

"I slowly eased my way into this field during grad school, she says. "I started studying cyberwarfare, which tied in perfectly with my intelligence analyst background. I loved learning about new technologies and hackers trying to attack corporations and countries."

She is of the opinion that most cybersecurity companies allow you to work remotely, but the downside is you don't get to physically see the people



ANDREA CARTER SENIOR DIRECTOR, MARKETING, NORTH, SOUTH AND EMERGING EMEA, SOPHOS



CIARA CAMPBELL, SECURITY ENGINEER, TENABLE

you work with; it may be months or sometimes never. "The best part about this field is that you get to attend some of the best conferences, gain some of the most sought-after skills, and work with some of the smartest people ever. I love it here!"

HACKERS HAVE THEIR EYE ON THESE UAE INDUSTRIES

NICOLAI SOLLING, CHIEF TECHNOLOGY OFFICER, HELP AG

very crucial reality of today's hyperconnected world is that devices and systems share a global risk of exposure. The obscure exploit "Log4j" served as a much-needed wake-up call as it got global governments, enterprise businesses, leading tech companies and cybersecurity agencies scrambling to protect their infrastructure, systems and devices while managing the risks it posed.

Log4j, part of a Java logging library used by millions of computers worldwide to record errors and routine system operations, usually sends diagnostic messages about them to system administrators and users. But in December 2021, a vulnerability (CVE-2021-44228) in the software allowed cyber attackers to remotely execute code and gain access to systems that use Log4j.

The initial disbelief worldwide soon gave way to intense investigations – revealing significant exposure across internet-facing systems, leading the director of the United States' Cybersecurity and Infrastructure Agency CISA, Jen Easterly, to describe the vulnerability as the "most serious" she had ever seen in her entire career.

The case study of Log4j represents one of the most potent cybersecurity lessons of our time. It not only showcases the vulnerabilities that lurk around the so-



called safe areas of the cyberspace, but also exposes the lack of timely detection of cyberthreats targeting specific industries, sectors, and companies. As businesses in the region and around the world move with a ravenous appetite to seize the opportunities offered by new technology, one of the pitfalls has been a false sense of security that has left them vulnerable to cyber attacks.

In the UAE, as Help AG's State of the Market Report 2022 reveals, cyber attackers are becoming more professional and targeting organisations strategically, particularly government entities – being a target of 37% of Distributed Denial-of-Service (DDoS) attacks. This is followed by the private sector (34%), healthcare operators (8%), financial companies (6%), the education sector (5%), oil, gas and energy companies (4%), and the hospitality segment (4%) – highlighting a landscape where almost every major pillar of the economy is prone to cyber attacks in the absence of a robust security protocol.

Government sector

With the UAE and Gulf countries in the midst of a strategic transformation into a knowledge economy, embracing new technologies presents both an opportunity and a threat. The vulnerabilities that governments are exposed to in the region, as per the State of the Market Report 2022, mirror global findings – be it in terms of DDoS attacks, cloud threats, ransomware or critical vulnerabilities in common applications.

The resilience of governments and economies will depend on the collective action of businesses and individuals – which can only be achieved by creating a strong business continuity plan with cybersecurity controls at every step, along with having a well-structured incident response and recovery plan in place, coupled with acknowledging that cybersecurity is everyone's responsibility.

Healthcare industry

The COVID-19 pandemic led to a decisive shift towards telehealth and

WITH THE UAE AND GULF COUNTRIES IN THE MIDST OF A STRATEGIC TRANSFORMATION INTO A KNOWLEDGE ECONOMY, EMBRACING NEW TECHNOLOGIES PRESENTS BOTH AN OPPORTUNITY AND A THREAT.

telemedicine, thereby increasing the risks for breaches of sensitive data and medical records, and putting the spotlight on how patient information is shared across employees. Other unique cybersecurity dangers faced by the sector include remote attacks on healthcare facilities resulting in the takeover of medical devices and the denial of vital, life-saving services. Protecting the confidentiality and availability of information, and securing the different entry points while replacing legacy systems must therefore be a top priority for companies in the healthcare sector.

Banks and financial institutions

Whether seeking a financial windfall or political leverage, banks and financial institutions are leading targets of cybercriminals globally, and the UAE is no exception. The stakes are especially high in the sector since it is not just banks and financial systems that could be compromised, but entire economies that could be crippled or disrupted.

It is therefore imperative for such institutions to ramp up their cyber vigilance, especially as the UAE and other Gulf countries move towards a digital economy and increasingly cashless transactions. Not embedding cybersecurity by design in the banking sector can not only compromise customer data and loyalty, but recovering from such breaches can incur huge costs and be very difficult.

Educational sector

Yet another core sector that needs to make cybersecurity a priority is education. Cybercrimes seem to be gaining ground every year as schools and higher education increasingly embrace a hybrid model, with online systems being targeted, malware attacks holding up classes and even student safety coming under increasing attack. That is why it is imperative for educational institutions to adopt a comprehensive cybersecurity strategy that allows them to assess, defend, and respond effectively and in a timely manner without compromising user experience.

Oil, gas and energy companies

As oil, gas and energy companies adopt digitalisation of technologies and operations with increased information technology (IT) and operational technology (OT) convergence, they are faced with an expanding attack surface that continues to present entry points to their previously isolated systems, thus impacting their visibility and placing them among the most vulnerable sectors to cyberthreats. Oil and gas companies form a vital part of any national energy infrastructure, and they simply cannot afford to compromise on their digital security requirements. In many cases, there could be a need to revamp the entire security estate with state-of-theart technologies and ultimately change the approach to managing and mitigating cyberattacks by leading with AI-based threat detection and response.

From cybersecurity to cyber resilience

A hyperconnected world with key verticals of the economy integrated with and dependent on each other puts all IT systems in a shared risk of exposure and demands a comprehensive approach to move from cybersecurity to cyber resilience. With a trusted security partner, sophisticated solutions and best-in-class services, along with a transformed culture around cybersecurity, this journey can happen seamlessly for organisations in the long run – and the time to start on it is now. **1**



SECURING THE IOT LANDSCAPE

MARCUS JOSEFSSON, VICE PRESIDENT SALES, NOZOMI NETWORKS, TELLS SECURITY ADVISOR ALL ABOUT IOT SECURITY AND HOW THE COMPANY IS FOCUSED ON HELPING REGIONAL ORGANISATIONS WITH CRITICAL IOT NETWORKS.

ell us the latest findings of the Nozomi Networks Labs report.

Our latest OT/IoT security report found that in the first half of 2022, the threat landscape was disrupted by wiper malware, IoT botnet activity, and the Russia/Ukraine war.

We have observed activity from a variety of threat actors – hacktivists, nation-state APTs, and cybercriminals – since Russia began its invasion of Ukraine in February 2022. There has been a robust usage of wiper malware and the emergence of Industroyer2, a form of malware designed to abuse the IEC-104 protocol, commonly used in industrial environments.

Moreover, malicious IoT botnet activity increased and grew in sophistication. Our researchers set up a series of honeypots to attract these malicious botnets and capture their activity to provide additional insights into how threat actors target IoT. From January to June 2022, these honeypots discovered:

- March was the most active month with close to 5,000 unique attacker IP addresses collected.
- The top attacker IP addresses were associated with China and the United States.
- "root" and "admin" credentials were most often targeted and used in multiple variations as a way for threat actors to access all system commands and user accounts.

This research uncovered growing security concerns for both hard-coded passwords and internet interfaces for end-user credentials.

In terms of vulnerability, manufacturing, energy, healthcare and commercial facilities remain the most vulnerable industries.

Today, many organisations lack the ability to monitor and secure their IoT devices. How does Nozomi Networks step in?

The widespread deployment of IoT

technologies has created OT monitoring and security challenges for several organisations. Our offerings analyse all ICS, OT and IoT devices on the network for cyber threats, identifies security gaps, and helps close them.

Our Vantage SaaS solution, for one, was specifically designed to scale across multiple sites containing a large number of IoT devices and leverages the power and simplicity of the cloud to deliver unprecedented security and visibility across an organisation's OT, IoT, and IT networks. It displays all assets communicating on one network for real-time awareness, summarising all asset activity for rapid assessment. Immediate visualisation of all devices on a network enables continuous central monitoring of networks and automation systems from anywhere in the world, effectively eliminating blind spots and increasing cyber threat awareness.

Organisations can quickly detect and disrupt cyber risks and anomalies



with Vantage as it provides an automated vulnerability assessment and detailed risk information including security alerts and missing patches.

Additionally, our Smart Polling software uses a powerful combination of active and passive asset discovery for enhanced IoT device tracking, vulnerability assessment and security monitoring to help identify guaranteed vulnerabilities before they're exploited. It also identifies rogue devices and assets that don't belong in a particular environment.

What is the greatest challenge faced by organisations when it comes to IoT security?

The adoption of IoT technology has created several visibility and security challenges for organisations. Currently, the most predominant one for organisations is securing and monitoring IoT assets well without business interference. As industrial organisations deploy 5G with the capacity to support innumerable IoT assets in their global operations, these risks will only grow.

As IoT usage surges, attack surfaces and the volume of data and devices

that need to be monitored also expand. Industrial organisations are finding it harder to scale, because their onpremises monitoring and security technologies lack the capacity to analyse the data generated by the widespread deployment of IoT sensors. The deployment of IoT devices creates new challenges for security teams, including vulnerable firmware, weak default passwords, limited endpoint protection, and more.

Ongoing OT/IT convergence is accelerating the consolidation of two formerly separate networks and additionally creating risks. Increased access between OT networks and internet-facing IT networks means that centralised security and operations teams are struggling to monitor these environments using technology designed either for IoT or IT. Consequently, threat actors then take advantage of these security blind spots to target OT and IoT devices more frequently.

What is the company's plan for the region, going forward?

We will continue to grow and develop

our team in the Middle East to allow us to continue providing the level of service we currently do. Our focus will continue to be on helping regional organisations with critical national infrastructure and critical IoT networks to build a solid cybersecurity framework, taking into consideration local regulations. Nozomi Networks continues to see the convergence between IT and OT and the challenges associated with it, alongside the proliferation of IoT devices joining networks that need securing.

How does Nozomi work with its global strategic alliances to optimise IT & OT security

Nozomi Networks has established itself as a global leader in OT & IoT Security whilst partnering with global OEMs (alliances) to provide end to end OT & IoT solutions. Our partner-first together with a world class go-to-market strategy allows us to identify and recruit some of the best partners in the industry, ones that continuously innovating and providing best in class OT & IoT security solutions and services. **1**



DISPLAY & CONTROL SOLUTIONS WITH PRESENTATION MATRIX & SCALER



Hikvision is the world's leading IoT provider with video as its core competency, commercial display business also being its key focus area. Malco Technologies is an official Hikvision Displays distributor in the UAE, offering LED/LCD Video Walls, digital signage and 3D/transparent screens to suit every Boardroom, Media advertising, NOC/SOC control room requirements. By pairing with Kramer's Matrix switchers, VIA Connect PRO Wireless Collaboration Solution and Video Wall Controller etc. the applications are unlimited.







enquiry@mbal.ae www.malcotechnology.com LinkedIn.com/@MalcoTechnologies Facebook.com/@MalcoTechnologies Instagram.com/@Malco_Technologies Twitter.com/@MalcoTechnolog1

Business Bay, #014, 801 P.O.Box: 6257, Dubai, UAE

LEGACY TECHNOLOGY UNDERMINES RANSOMWARE RESPONSE

ew global research commissioned by Cohesity, a leader in next-gen data management, reveals that nearly half of respondents say their company depends on outdated, legacy backup and recovery infrastructure to manage and protect their data. In some cases, this technology is more than 20 years old and was designed long before today's multicloud era and onslaught of sophisticated cyberattacks plaguing enterprises globally.

Challenges pertaining to outdated infrastructure could easily be compounded by the fact that many IT and security teams don't seem to have a plan in place to mobilise if and when a cyberattack occurs. Nearly 60% of respondents expressed some level of concern that their IT and security teams would be able to mobilise efficiently to respond to an attack.

"IT and security teams should raise the alarm bell if their organisation continues to use antiquated technology to manage and secure their most critical digital asset – their data," said Brian Spanswick, Chief Information Security Officer, Cohesity. "Cyber criminals are actively preying on this outdated infrastructure as they know it was not built for today's dispersed, multicloud environments, nor was it built to help companies protect and rapidly recover from sophisticated cyberattacks."

Backup and Recovery Infrastructure That Could Be Considered Archaic

Forty-six percent of respondents said that their organisation relies on primary backup and recovery infrastructure that was designed in, or before, 2010. Nearly 100 respondents (94 out of 2011) revealed that their organisation relies on backup and recovery infrastructure that was built before the new millennium — in the 1990s.

Enterprises are utilising this legacy technology despite the fact that managing

and securing data environments has become much more complex, not just because of the exponential growth in structured and unstructured data, but because of the vast array of locations where that data is stored. Forty-one percent of respondents stated that they store data onpremises, 43% rely on public cloud storage, 53% utilise a private cloud, and 44% have adopted a hybrid model (some respondents are using more than one option).

"In 2022, the fact that any organisation is using technology to manage their data that was designed in the 1990s is frightening given that data can be compromised, exfiltrated, held hostage, and it can create massive compliance issues for organisations," said Spanswick. "In this survey, we found nearly 100 respondents who said their organisations are relying on outdated data infrastructure, and this raises the question, how many other businesses are in the same situation around the world?"

What Keeps IT and SecOps Teams Up at Night

Respondents highlighted what they believe would be their biggest barriers to getting their organisation back up and running after a successful ransomware attack. The findings are as follows (respondents were asked to check all that apply):

- integration between IT and security systems (41%)
- lack of coordination between IT and Security (38%)
- lack of an automated disaster recovery system (34%)
- antiquated backup and recovery systems (32%)
- lack of a recent, clean, immutable copy of data (32%)
- lack of and timely detailed alerts (31%) With respect to the lack of coordination between IT and security, this coincides with other findings from this survey denoting that a gap often exists between IT and SecOps that puts businesses and security postures at risk.



What Do Survey Respondents Want Management to Prioritise

Respondents revealed that modernising data management, protection, and recovery capabilities, in addition to increasing collaboration between IT and SecOps, offers a path to strengthening their organisations' security postures and multicloud operations. The top five "must have" measures that respondents would ask management for in 2022 are:

- Integration between modern data management and security platforms and Al-powered anomalous data access alerts to provide early warning of attacks in progress (34%)
- Extensible platform for third-party applications for security operations and incident response (33%)
- Automated disaster recovery of systems and data (33%)
- Upgrading from legacy backup and recovery systems (32%)
- Rapid, organisation-wide backup with in transit data encryption (30%)

"Both IT decision-makers and SecOps should co-own the cyber resilience outcomes, and this includes an evaluation of all infrastructure used in accordance with the NIST framework for data identification, protection, detection, response, and recovery. Also, both teams need to have a comprehensive understanding of the potential attack surface," said Spanswick. "Next-gen data management platforms can close the technology gap, improve data visibility, help IT and SecOps teams sleep better at night, and stay one step ahead of bad actors who take great delight in exfiltrating data from legacy systems that can't be recovered." 1

GLOBAL DEV SLAM 10-13 OCT 2022 DUBAI WORLD TRADE CENTRE



^مقر المبرمجين coders (hq)

Featuring the inaugural



POWERING CODING INGENUITY

THE WORLD'S LARGEST MEET UP FOR

THE DEVELOPER & CODING COMMUNITY

TECH PIONEERS ON STAGE



Travis Oliphant Creator of NumbPy & Co-Founder





Ketan Umare Co-Creator of Flyte, Co-Founder & CEO





Sebastian Ramirez Montano Creator

FastAPI Germany

Pablo Galindo Salgado Physicist & Software Engineer - R&D Python Infrastructurea

Bloomberg UK

DON'T MISS OUT, GET YOUR DELEGATE PASS



For delegate group booking, call Fahad Khalife at: +971 4 308 6805 | globaldevslammarketing@dwtc.com G L O B A L D E V S L A M . C O M # G L O B A L D E V S L A M

Founding Partners









Gold Sponsor



Silver Sponsor



hat does the regional threat/security landscape look like? Unsurprisingly, the

rapid digitisation of industries in the region is continuing to expand opportunities for threat actors to launch attacks. Now more than ever, email and collaboration are where work happens and it is the key way by which we connect our communications, our people, and our data. Our work surface has now become the greatest concentration of risk.

Our latest State of Email Security 2022 research found that email usage had increased at more than eight out of ten companies in Saudi Arabia and the UAE, with 46% saying the increase was significant.

Email-based threats are also on the rise and remains the biggest threat vector, with more than two-thirds of UAE companies saying they've received an increased number of email-based threats in the past year.

Saudi Arabian companies are also displaying encouraging resilience against ransomware. While 60% of companies in the country were hit by a ransomware attack, the average downtime following a successful attack was only five days compared to a global average of over seven, while seventeen percent of companies said they experienced no downtime at all, well ahead of a global average of only 2% of companies that could claim the same.

Tell us about the Mimecast X1 platform.

The Mimecast X1 Platform is the foundation of the broader Mimecast Product Suite, designed to mitigate risk

SECURING E-MAILS

ANITA JOSEPH CAUGHT UP WITH **WERNO GEVERS**, REGIONAL DIRECTOR AT MIMECAST MIDDLE EAST, TO FIND OUT MORE ABOUT THE X1 PLATFORM AND HOW TO MITIGATE RISK ACROSS EMAIL COMMUNICATIONS. across email communications, and help empower organisations to secure their workplace environment - wherever work happens. Essentially, the X1 Platform is built to drive industry-leading detection capabilities, deliver reliability, resilience and scale, and transform data into insights that turn email and collaboration security into the eyes and ears of organisations.

The platform consists of four core innovations that are designed to mitigate risk and manage complexities, namely: **Mimecast X1 Precision Detection,** which applies the latest advancements in AI and machine learning to enable intelligent detection of emerging and unknown threat types while keeping users safe all the way down to the point of risk; **Mimecast X1 Service Fabric,** which provides the foundation for clouddelivered security at scale;

Mimecast X1 Data Analytics, which was built with one goal in mind: to make information actionable for customers; and Mimecast Extensible Security Hooks (MESH), which unlocks a vast API ecosystem that supports the fast, simplified integration of Mimecast with existing security investments spanning hundreds of third-party solutions.

As the top attack vector, email demands the strongest possible protection. Tell us how Mimecast secures emails against the most sophisticated attacks.

As the leader in email security for 20 years, Mimecast offers industry-leading detection and world-class efficacy trusted by 40,000 customers globally. By applying the right detection capabilities at the right time, we surround your communications

THE X1 PLATFORM IS BUILT TO DRIVE INDUSTRY-LEADING DETECTION CAPABILITIES, DELIVER RELIABILITY, RESILIENCE AND SCALE.



with continuous protection to block the most sophisticated threats. The industry's most robust view of the email threat landscape – derived from Mimecast's inspection of 1.3B emails daily – powers instantaneous blocking of most emailbased attacks, while the latest in AI and machine learning provides intelligent detection of both emerging and unknown threat types.

Our system starts with a foundation centred around where your work happens; a scalable cloud platform that connects into, understands, and learns from your communications, your people, and data to systematically enhance everything around it.

How does Mimecast use AI to enhance its security offerings?

Mimecast uses AI and machine learning models based on an analysis of more than 1.3 billion emails per day to filter out malicious emails at scale and drive the intelligent analysis of the 'unknown'.

Mimecast's CyberGraph solution utilises AI to protect from the most evasive and hard-to-detect email threats, limiting cyberattackers' reconnaissance capabilities and mitigating human error. This includes email tracker prevention, identity graph technology that detects anomalous behaviour that could point to malicious activity, and misaddressed email protection to identify and prevent accidental data loss caused by employees sending emails to the incorrect recipient. Unlike rules-based policies, CyberGraph continually learns and requires almost no configuration, lessening the burden on IT teams and reducing the likelihood of misconfiguration that could lead to security incidents.

In your opinion, what type of organisation is best positioned to leverage AI for security: enterprises, or security vendors and why?

Organisations from all sizes and industries can and should leverage AI. Despite the complex algorithms under the hood, the benefits of AI are straightforward and easy to articulate. AI can process huge data volumes — much more than humans could make sense of. It processes information far quicker than a human, and makes smarter decisions over time, so long as there's a data science team in place to monitor and retrain the AI models as needed.

Applied to cybersecurity, where data volumes are large and a few extra minutes of response time can mean the difference between blocked attack and disastrous breach, those benefits can create tremendous enterprise value. Capgemini research found that 75% of responding executives from global organizations said AI allows their organisation to respond faster to breaches. Unsurprisingly, 69% also believe AI is necessary for an effective response to a cyberattack. **1**

MANAGING SECURITY

ANITA JOSEPH CAUGHT UP WITH **AJAY NAWANI**, DIRECTOR -SALES ENGINEERING, MEA AT SOPHOS TO FIND OUT MORE ABOUT RANSOMWARE, MDR & THREAT INTELLIGENCE.

hat is the cybersecurity landscape like today? Are there any new threats we must be aware of? Globally, we have seen

cyberthreats becoming more interrelated targeting an interrelated world. The Sophos 2022 Threat Report shows how the gravitational force of ransomware's black hole is pulling in other cyberthreats to form one massive, interconnected ransomware delivery system – with significant implications for IT security.

Sophos' The State of Ransomware 2022 survey also shows that ransomware is a big problem for the UAE organisations. Fifty-nine percent of UAE organisations surveyed were hit with ransomware in 2021, up from 38% in 2020.

Ransomware shows no sign of slowing down, though its business model is continuously shifting towards Ransomware-as-a-service and is expanding, with Initial Access Brokers (IABs) selling network access to any potential ransomware attacker. Even "unskilled hackers" can get into the ransomware business – by buying the network access, encryption code and other bespoke pieces need to do so.

Sophos believes that, in 2022 and beyond, the RaaS business model will continue to dominate the threat landscape for ransomware attacks, as this model permits experts in ransomware construction to continue to build and improve their product.

The rise of ransomware brokers and the continued talent shortage mean defenders increasingly need security technology managed on their behalf. So how important is the need for Managed Security Services today?

Cybersecurity has become so complex that organisations cannot do it alone. There is an ever-increasing escalation of cyberattacks



incidents. And there is a cybersecurity skill gap that every organisation is facing at some level. This skills gap is in a way helping adversaries to escalate cyberattacks.

Cybersecurity is a 24/7 job; attackers often strike on weekends, during holidays or after hours, when a network could be less monitored. People are also feeling burnt out from needing to work around the clock to defend against attacks, especially during Covid, when the line separating work and personal time became extra blurry.

Sophisticated attacks like ransomware are often the last sign an adversary has breached an organisation's network. In fact, when it's obvious that a business has been victimised by a ransomware attack, it typically means cybercriminals have been lurking for days, if not months.

Every ransomware attack has indicators of compromise along the attack chain. To recognise them, organisations need trained human experts, along with next generation protection, detection and response defenses.

Outsourcing cybersecurity requirements to an expert that provides it as a service can help organisations of all sizes with a fully managed service to deal with any cyber issues 24x7 365 days of the year. It helps organisations to have the right tools, people and processes to effectively provide the active threat protection their business needs. It also helps organisations to proactively hunt for threats, scope their severity, initiate action, and provide actionable advice to address the root cause of incidents.

Engaging an external cybersecurity team also saves the hiring headache of having to find experts with the right skills, onboarding and training, as well as ensuring these employees are staying on top of the ever-evolving threat landscape.

Cybersecurity as a service helps organisations continuously evaluate their cybersecurity strategy and quickly make adjustments as required to ensure the

OUTSOURCING CYBERSECURITY REQUIREMENTS TO AN EXPERT CAN HELP ORGANISATIONS WITH A FULLY MANAGED SERVICE TO DEAL WITH ANY CYBER ISSUE 24X7, 365 DAYS OF THE YEAR.

level of protection is proportionate to their respective risk profiles.

Tell us about Sophos MDR-How's it different from the other MDR offerings in the market?

Sophos MDR is different in the following ways:

Sophos MDR takes action: Sophos MDR not only just monitors and notify when suspicious activity is detected it takes action. We remotely initiate actions to disrupt, contain, and neutralise even the most sophisticated threats.

Elite expertise: With over 10,000 customers, Sophos has seen it all and stopped it all. Our highly trained team of threat hunters, engineers, and ethical hackers has your back 24/7, investigating anomalous behaviour and taking action against threats.

Robust threat hunting: Sophos conducts lead-driven and lead-less threat hunts to discover new Indicators of Attack (IoA) and Indicators of Compromise (IoC) that previously could not be detected.

High-fidelity detections: Going beyond traditional detections, Sophos combines deterministic and machine learning models to spot suspicious behaviors and the tactics, techniques and procedures used by the most advanced adversaries.

Sophos recently announced X-Ops, a new cross-operational unit linking SophosLabs, Sophos SecOps and Sophos AI. Tell us more.

Sophos X-Ops links SophosLabs, Sophos SecOps and Sophos AI, three established teams of cybersecurity experts at Sophos, to help organisations better defend against constantly changing and increasingly complex cyberattacks. Sophos X-Ops leverages the predictive, real-time, real-world, and deeply researched threat intelligence from each group, which, in turn, collaborate to deliver stronger, more innovative protection, detection and response capabilities.

Sophos X-Ops is gathering and operating on threat intelligence from its own multidisciplinary groups to help stop attackers earlier, preventing or minimising the harms of ransomware, espionage or other cybercrimes that can befall organisations of all types and sizes, and working with law enforcement to neutralise attacker infrastructure. While Sophos' internal teams already share information as a matter of course, the formal creation of Sophos X-Ops drives forward a faster, more streamlined process necessary to counter equally fast-moving adversaries.

Sophos X-Ops also provides a stronger cross-operational foundation for innovation, an essential component of cybersecurity due to the aggressive advancements in organised cybercrime. By intertwining the expertise of each group, Sophos is pioneering the concept of an artificial intelligence (AI) assisted Security Operations Center (SOC), which anticipates the intentions of security analysts and provides relevant defensive actions. In the SOC of the future, Sophos believes this approach will dramatically accelerate security workflows and the ability to more quickly detect and respond to novel and priority indicators of compromise. 1



Be Part of the History as You Watch the World's Most Exciting Sports Game, Live Onscreen with the **136**" All-in-One Display

The 136 large screen which is offered as an all-in-one package including an embedded controller and built-in speaker. Not only it is easy to install, it gives even better when all you need to do is to turn on the screen with a remote control and enjoy like a home TV.







(())





Compatible with TV Box Cloudflare is a Leader in the 2022 Gartner[®] Magic Quadrant[®] for WAAP

CLOUDFLARE NAMED A LEADER BY GARTNER

artner has recognised Cloudflare as a Leader in the 2022 "Gartner Magic Quadrant for Web Application and API Protection (WAAP)" report that evaluated 11 vendors for their 'ability to execute' and 'completeness of vision'. This achievement highlights Cloudflare's continued commitment and investment in this space as the company aims to provide better and more effective security solutions to its users and customers.

Keeping up with application security

With over 36 million HTTP requests per second being processed by the Cloudflare global network, the company gets unprecedented visibility into network patterns and attack vectors. This scale allows it to effectively differentiate clean traffic from malicious, resulting in about 1 in every 10 HTTP requests proxied by Cloudflare being mitigated at the edge by the WAAP portfolio. Visibility is not enough, and as new use cases and patterns emerge, Cloudflare invests in research and new product development. Cloudflare's continued investment in application security has helped it gain it's position in this space.

Cloudflare WAAP

Cloudflare has built several features that fall under the Web Application and API

Protection (WAAP) umbrella.

DDoS protection & mitigation

Cloudflare's network, which spans more than 275 cities in over 100 countries is the backbone of its platform, and is a core component that allows mitigation of DDoS attacks of any size. To help with this, the company's network is intentionally anycasted and advertises the same IP addresses from all locations, allowing it to "split" incoming traffic into manageable chunks that each location can handle with ease, and this is especially important when mitigating large volumetric Distributed Denial of Service (DDoS) attacks..

Web Application Firewall

Cloudflare's WAF is a core component of its application security and ensures hackers and vulnerability scanners have a hard time trying to find potential vulnerabilities in web applications. This is very important when zero-day vulnerabilities become publicly available as bad actors attempt to leverage new vectors within hours of them becoming public. Cloudflare's WAF comes packed with many advanced features such as leaked credential checks, advanced analytics and alerting and payload logging.

Bot Management

It is no secret that a large portion of web traffic is automated, and while not all

automation is bad, some is unnecessary and may also be malicious.

The company's Bot Management product works in parallel to its WAF and scores every request with the likelihood of it being generated by a bot, allowing organizations to easily filter unwanted traffic by deploying a WAF Custom Rule, all this backed by powerful analytics. Cloudflare make this easy by also maintaining a list of verified bots that can be used to further improve a security policy. In the event of wanting to block automated traffic, Cloudflare's managed challenge ensures that only bots receive a hard time without impacting the experience of real users.

API Gateway

API traffic, by definition, is very wellstructured relative to standard web pages consumed by browsers. At the same time, APIs tend to be closer abstractions to back end databases and services, resulting in increased attention from malicious actors and often go unnoticed even to internal security teams (shadow APIs).

Page Shield

Attacks that leverage the browser environment directly can go unnoticed for some time, as they don't necessarily require the back-end application to be compromised. Page Shield is solving client side security by providing active monitoring of third party libraries and alerting application owners whenever a third party asset shows malicious activity. It leverages both public standards such as content security policies (CSP) along with custom classifiers to ensure coverage.

Security Center

Cloudflare's new Security Center is the home of the WAAP portfolio. A single place for security professionals to get a broad view across both network and infrastructure assets protected by Cloudflare. oving forward the plan is for the Security Center to be the starting point for forensics and analysis, allowing companies to also leverage Cloudflare threat intelligence when investigating incidents.



10-14 OCT 2022 DUBAI WORLD TRADE CENTRE

SHOW TIMINGS: 10 Oct - 11am to 5pm | 11 - 14 Oct - 10am to 5pm

THE WORLD'S LARGEST & MOST INFLUENTIAL TECH + STARTUP EVENT



ATTENDEES BADGE SPONSOR



CITY

SILVER SPONSOR

ManageEngine

a division of Zoho Corp.

DUBAI INTERNET CONNEXIONS LOUNGE SPONSOR



midis

MAJLIS LOUNGE SPONSOR





RETAIL INDUSTRY SECOND MOST TARGETED BY RANSOMWARE IN 2021

Chester Wisniewski

ophos, a global leader in next-generation cybersecurity, has published a new sectoral survey report, The State of Ransomware in Retail 2022, which found that retail had the second highest rate of ransomware attacks last year of all sectors surveyed after the media, leisure, and entertainment industry. Globally, 77% of retail organisations surveyed were hit—a 75% increase from 2020. This is also 11% more than the cross-sector average attack rate of 66%.

"Retailers continue to suffer one of the highest rates of ransomware attacks of any industry. With more than three in four suffering an attack in 2021, it certainly brings a ransomware incident into the category of when, not if. In Sophos' experience, the organisations that are successfully defending against these attacks are not just using layered defenses, they are augmenting security with humans trained to monitor for breaches and actively hunting down threats that bypass the perimeter before they can detonate into even bigger problems. This year's survey shows that only 28% of retail organisations targeted were able to stop their data from being encrypted, suggesting that a large portion of the industry needs to improve their security posture with the right tools and appropriately trained security experts to help manage their efforts," said Chester Wisniewski, principal research scientist, Sophos.

As the percentage of retail organisations attacked by ransomware increased, so did the average ransom payment. In 2021, the average ransom payment was \$226,044, a 53% increase when compared to 2020 (\$147,811). However, this was less than one-third the cross-sector average (\$812K).

"It's likely that different threat groups are hitting different industries. Some of the low-skill ransomware groups ask for \$50,000 to \$200,000 in ransom payments, whereas the larger, more sophisticated attackers with increased visibility demand \$1 million or more." said Wisniewski. "With Initial Access Brokers (IABs) and Ransomware-as-a-Service (RaaS), it's unfortunately easy for bottom-rung cybercriminals to buy network access and a ransomware kit to launch an attack without much effort. Individual retail stores and small chains are more likely to be targeted by these smaller opportunistic attackers," said Wisniewski. Additional findings include:

- While the retail sector was the second most targeted industry, the perceived increase in the volume and complexity of cyberattacks against the industry were slightly below the cross-sector average (55% and 55% respectively).
- 92% of retail organisations hit by ransomware said the attack impacted their ability to operate and 89% said the attack caused their organisation to lose business/revenue
- In 2021, the overall cost to retail

organisations to remediate a ransomware attack was \$1.27M, down from \$1.97M in 2020.

 When compared to 2020, the amount of data recovered after paying the ransom decreased (from 67% to 62%), as did the percentage of retail organisations that got all their data back (from 9% to 5%).

In the light of the survey findings, Sophos experts recommend the following best practices for all organisations across all sectors:

- Install and maintain high-quality defenses across all points in the environment. Review security controls regularly and make sure they continue to meet the organisation's needs.
- Proactively hunt for threats to identify and stop adversaries before they can execute attacks – if the team lacks the time or skills to do this in-house, outsource to a Managed Detection and Response (MDR) team.
- Harden the IT environment by searching for and closing key security gaps: unpatched devices, unprotected machines and open RDP ports, for example. Extended Detection and Response (XDR) solutions are ideal for this purpose.
- Prepare for the worst, and have an updated plan in place of a worst-case incident scenario
- Make backups, and practice restoring them to ensure minimal disruption and recovery time. 1





Simple. Powerful. **Secure IT.**

- Over 300,000 customers in 190 » countries from SMB to Fortune 500[®]
- 499 of the Fortune 500 are customers »
- #1 in Network Management* »
- 50+ IT management products »

solarwinds.com

* IDC Worldwide Network Management Software Tracker 2H 2020.

Come visit us at GITEX!

October 10 - 14 | Dubai | H7-F30

















APPLICATION MANAGEMENT

MANAGEMENT

SYSTEMS MANAGEMENT MANAGEMENT



IT SECURITY

Switching that Stacks Above the Competition

Highly Scalable Solutions for a Future-Proof Enterprise Network



Future-proof your network with 100G uplink port speeds

Virtual Switching Unit (VSU) • Enterprise Layer 3 Features

Advanced Quality of Service (QoS)



Connect to more...

https://me.dlink.com