ISSUE 51 | SEPTEMBER 2020 WWW.TAHAWULTECH.COM





REVIEW:

SEAGATE SKYHAWK AI

EXPERT'S CORNER:

THE DAWN OF THE BUSINESS-**ALIGNED SECURITY EXECUTIVE**

IN DEPTH DEFENCE

MIMECAST'S

HOW TO

GET THE BEST VALUE OUT OF SECURITY **ASSESSMENTS**

CHANGIN

HOW CYBEREASON'S OFFENSIVE AND OPERATIVE APPROACH IS TRANSFORMING CYBERSECURITY STRATEGIES

EXCUSIVE INTERVENT



SUPPLEMENT



Video Based Smart Campus

Campus Security, Real-time tracking, Proactive alarm



Situation Awareness Video-based Perimeter Video-based Patrol

Video based Personnel and Vehicle management



FR-based Access

Vehicle Access Control



Contact Us: e.huawei.com/ae enterpriseME@huawei.com

CONTENTS











How secure Are We?

Tenable on why organisations need to align their business and security strategies

24 THE FUTURE OF SMART SECURITY

WD on how the rising demands for Al- and 4K-enabled smart video cameras are driving storage needs 28 UNLOCKING THREAT INTELLIGENCE

How Cyware is enabling organisations leverage the strategic value of threat intelligence

REVIEW: SEAGATE SKYHAWK AI
Why Seagate's SkyHawk AI HDDs are
the perfect answer to today's video
surveillance storage needs



SD-WAN can deliver reduced WAN costs. But it can't be at the expense of Security.

Fortinet's Secure SD-WAN solution provides full SD-WAN capabilities with all of the Next Generation Security features needed for today's ever-changing threat landscape.



www.fortinet.com



EDITORIAL



Talk to us: E-mail: adelle.geronimo@ cpimediagroup.com

Adelle Geronimo

EVENTS





A WHOLE NEW WORLD

VALUE OF

The COVID-19 pandemic is changing everything.

More than social distancing, constant sanitation, stricter border rules and fragmented workforces, the pandemic is pushing organisations to be more digital. However, the digital response to the crisis has created new vulnerabilities, which made them rethink their security strategies.

As many countries relax the guarantine

measures, businesses are starting to reopen and they face the challenge of implementing new policies and tools to protect the growing number and diversity of devices connecting to networks. In the Middle East, the cybersecurity market size is projected to grow from \$15.6 billion in 2020 to \$29.9 billion **MIDDLE EAST'S** by 2025, according to the latest data **CYBERSECURITY** by ResearchandMarkets. This is **MARKET BY 2025** primarily driven by the rising security breaches and sophisticated cyber-attacks across enterprises and critical industries in the region. Additionally, the changing landscape is also pushing technology providers to evolve their strategies and offerings to accommodate

This issue features interview with a number of key industry players who have shared insights on how business leaders can emerge successful despite the challenges including Mimecast's

enterprises and help them adapt in the new era.

Werno Gevers who revealed the latest findings of the company's State of Email Security report. According to Gevers, users today are increasingly becoming vulnerable to phishing and social engineering attacks as they become desperate to get more information about the COVID-19 crisis.

On the cover is Cybereason's CEO and Co-Founder Lior Div, who discussed the company's journey to success and how their operative

> mindset and approach can enable enterprises gain an edge against the bad guys. He also highlighted the company's diverse and inclusive culture, which is truly inspiring.

Furthermore, this month's issue also features an inclusive interview with world-renowned ethical hacker and cybersecurity expert Bryan Seely

who delved into how he famously wiretapped the FBI and Secret Service using a vulnerability on Google Maps.

The world might never be the same again after the COVID-19 pandemic. But the best thing we can do is gather as many information as we can to better adapt and stay protected in this new world of threats.

We hope you enjoy reading the latest issue of Security Advisor ME!

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



Publishing Director Natasha Pendleton natasha.pendleton@cpimediagroup.com +971 4 440 9139

ADVERTISING **Group Sales Director** Kausar Syed kausar.syed@cpimediagroup.com +971 4 440 9130

Senior Sales Manager Sabita Miranda sabita.miranda@cpimediagroup.com +971 4 440 9128

EDITORIAL Online Editor

Adelle Geronimo adelle.geronimo@cpimediagroup.com +971 4 440 9135

Contributing Editor Mark Forker mark.forker@cpimediagroup.com +971 4 440 9153

DESIGN Senior Designer Analou Balbero analou.balbero@cpimediagroup.com +971 4 440 9140

> DIGITAL SERVICES Web Developer Jefferson de Jova

webmaster@cpimediagroup.com +971 4 440 9100

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

> Tel: +971 4 440 9100 Fax: +971 4 447 2409

Printed by Emirates Printing Press LLC, Dubai

> © Copyright 2020 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.

MIMECAST REDEFINES PHISH TESTING AND TRAINING WITH SAFE PHISH

Mimecast phishing has announced an

industry changing capability that will allow customers to launch live phishing simulations. Known as SAFE Phish, it's designed to let security teams create training exercises using real-life, deweaponised campaigns that target their organisations and employees. Training results are engineered to be incorporated into the Mimecast SAFE Score dashboard, which is designed to aggregate data to gauge a company's security posture. Organisations have an opportunity to re-define the way overall risk is measured as a result.

Michael Madon, SVP and GM of Mimecast Security Awareness Products, said, "With SAFE Phish technology, endusers can safely be exposed to real-life, de-weaponised phishing attacks to make training more effective and provide a data-driven picture of which employees are most at risk. Our research has shown that end-users who have taken Mimecast Awareness Training are 5.2 times less likely to click on dangerous links. We're very excited about how SAFE Phish simulations can further help increase the impact of our security awareness solution."

Because SAFE Phish results act as a security feed, data from phish testing can be incorporated into the Mimecast SAFE Score dashboard, which is designed to calculate individual user risk using four factors – engagement, knowledge, sentiment, and bad URL clicks. Data is also aggregated to provide an overall organisational risk assessment.

The Safe Score dashboard and SAFE Phish will be available in Q2 of FY 2021.



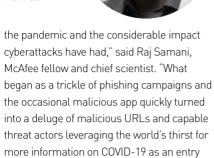
CYBERCRIMINALS LEVERAGE PANDEMIC AS ENTRY MECHANISM INTO SYSTEMS: MCAFEE REPORT

McAfee, the device-to-cloud cybersecurity

company, has released its McAfee COVID-19 Threat Report: July 2020 examining cybercriminal activity related to COVID-19 and the evolution of cyber threats in Q1 2020.

McAfee Labs saw an average of 375 new threats per minute and a surge of cybercriminals exploiting the pandemic through COVID-19 themed malicious apps, phishing campaigns, malware, and more. New PowerShell malware increased 688% over the course of the quarter while total malware grew 1,902% over the past four quarters. Disclosed incidents targeting the public sector, individuals, education and manufacturing increased; nearly 47% of all publicly disclosed security incidents took place in the United States.

"Thus far, the dominant themes of the 2020 threat landscape have been cybercriminal's quick adaptation to exploit RAJ SAMANI, MCAFEE



To track these campaigns, McAfee Advanced Programs Group (APG) has published a COVID-19 Threat Dashboard, which includes top threats leveraging the pandemic, most targeted verticals and countries, and most utilised threat types and volume over time. The dashboard is updated daily at 4pmET.

mechanism into systems across the globe."

QUALYS STRENGTHENS SECURITY AND THREAT RESEARCH OFFERINGS WITH LATEST ACQUISITION

Qualys has announced that it has acquired

the software assets of Spell Security, an endpoint detection and response start-up.

This acquisition further strengthens Qualys' security and threat research, advances endpoint behavior detection capabilities, and brings rich telemetry to the Qualys Cloud Platform. In addition, Spell's deep knowledge of threat hunting and adversary techniques provides unique defense capabilities and analysis addressing the multi-vector threats customers are now faced with.

As with all Qualys acquisitions, key Spell Security employees have joined Qualys, including founder Rajesh Mony as CTO of Malware Detection Solutions.

With native integration of Spell Security hunting and reporting capabilities on the

PHILIPPE COURTOT. QUALYS

Qualys platform, Qualys Multi-Vector EDR will enable security teams to detect and hunt for high fidelity threats, gain the full context of the attack path with powerful correlation of all security vectors for investigation and prioritisation of security incidents, and respond appropriately to eliminate the root cause of the incident.

Philippe Courtot, chairman and CEO of Qualys. "Adding Spell Security's technology to the Qualys Cloud Platform enables us to further strengthen our security and threat research, advanced endpoint behaviour detection and provide customers with enhanced telemetry for even greater visibility. We welcome Spell Security to the Qualys family."

HIKVISION POSTS \$3.475 BILLION IN REVENUES IN H1 2020

Hikvision, an IoT solution provider with

video as its core competency, has released its financial results for the first half of 2020. During the period, Hikvision generated a revenue of RMB 24.27 billion (\$3.475 billion) with a year-over-year (YoY) increase of 1.45 percent, and net profits attributable to shareholders of the company was RMB 4.62 billion (6.62 million), reflecting a YoY growth of 9.66 percent.

Hikvision's revenue in overseas markets achieved solid growth, amounting to RMB 7.54 billion (\$1.08 billion), with a YoY growth of 8.63 percent. Having encountered unusual global social and economic conditions in the first half of 2020, Hikvision adapted its operations and succeeded in making technological innovations meet customers' needs, which helped to overcome challenges and keep development steady. Hikvision will continuously work closely with its partners to maintain stable operations, create value for customers, and build more safety, efficiency and sustainability for communities around the world.

Key accounting data of Hikvision 2020 First Half Year Financial Results			
	2020 First Half Year	2019 First Half Year	YoY Change (%)
Operating income (RMB)	24,271,159,243.76	23,923,273,424.50	1.45%
Net profits attributable to shareholders of the company (RMB)	4,623,972,830.87	4,216,755,210.24	9.55%

FORTINET BOLSTERS CLOUD SECURITY CAPABILITIES WITH LATEST ACQUISITION

Fortinet has announced that it has acquired

OPAQ Networks, a Secure Access Service Edge (SASE) cloud provider based in Herndon, Virginia. OPAQ's Zero Trust Network Access (ZTNA) cloud solution protects organisations' distributed networks – from data centres, to branch offices, to remote users, and Internet of Things (IoT) devices.

Ken Xie, Founder, Chairman of the Board and CEO, said, "In this era of hyperconnectivity and expanding networks; with the network edge stretching across the entire digital infrastructure, networking and security must converge. In fact, the acquisition of OPAQ actually further enhances our existing SASE offering enabling Fortinet to deliver the most complete SASE platform on the market. The Fortinet SASE platform delivers the broadest security and industry-leading SD-WAN and networking offerings that can

all be delivered to customers and pa

all be delivered to customers and partners through a flexible, cost efficient and patented zero-trust cloud architecture."

Given remote workforce trends, with exponentially more users, devices, applications, services, and data outside of a traditional enterprise edge than inside, the integration of Fortinet's broad Security Fabric with OPAQ's cloud platform will

offer customers and partners even more choices in how they can consume best-of-breed security and is yet another unique and differentiated way Fortinet is empowering customers with the best, integrated security and networking innovation in real-time.

SECURELINK ANNOUNCES NEW STRATEGIC PARTNERSHIP WITH CIRCADENCE

REGHU MOHANDAS, SECURELINK

SecureLink,

a risk advisory firm based in

Dubai announced a

new strategic distribution partnership with Circadence – pioneers in handson, gamified and self-evaluating online cyber-learning that helps to build cybersecurity skills. Through this partnership, SecureLink aims to provide customers in the Middle East and Africa (META) with an innovative Al-based, next generation cybersecurity learning platform, Project Ares.

The partnership was born out of the market demands and challenges currently facing the cybersecurity community, namely the shortage of skilled professionals who seek hands-on skills training to keep pace with evolving threats. Circadence has responded to these dynamic challenges by delivering its award-winning gamified training and learning platform, Project Ares. The online cyber range learning solution helps cyber operators build and advance in skills and competencies.

Reghu Mohandas, Director – Risk Analytics & Advisory, SecureLink said, "Our relationship with Circadence brings to the region a true Gamified on-demand learning experience like no other.

Circadence provides an authentic

gamified learning environment which is optimised for

which is optimised for offense and defense trainings. Users will love the game-like experience and organisations can greatly improve retention rates while incorporating the "learn by doing" method for their users.

gamific whit of the state of th

SOURCE: MCAFEE LABS



HOW SECURE ARE WE?

Only the business-aligned cybersecurity leader can answer with confidence.



CYBERSECURITY NEEDS TO MATURE AS A BUSINESS RISK STRATEGY



of organizations experienced at least one business-impacting* cyberattack or compromise



of organizations expect an increase in cyberattacks over the next two years

THE BUSINESS IMPACT IS REAL



41%

Loss of customer and/or employee data



37%

Paid ransom following successful attack



35%

Suffered Financial loss or theft

SECURITY LEADERS STRUGGLE TO CLEARLY COMMUNICATE THEIR CYBER RISK POSTURE

Only four in 10 security leaders can answer the question "How secure or at risk are we?" with a high level of confidence.





THE DAWN OF THE **BUSINESS-ALIGNED SECURITY EXECUTIVE**

MAHER JADALLAH, REGIONAL DIRECTOR, MIDDLE EAST, TENABLE, SHARES INSIGHTS INTO WHY IT IS IMPERATIVE FOR ORGANISATIONS TO ALIGN THEIR BUSINESS AND SECURITY STRATEGIES

ybersecurity leaders often struggle to answer the question, "How secure are we?" According to a commissioned study conducted by Forrester Consulting on behalf of Tenable, just four out of 10 security leaders said they could answer the question, "How secure, or at risk, are we?" with a high level of confidence. And a whopping 66 percent of business leaders are - at most - only somewhat confident intheir security team's ability to quantify their organisation's level of risk or security.

So why is it so difficult?

Lack of holistic visibility

Today's digital environment is everchanging. Different types of assets constantly enter and exit the enterprise, and some are ephemeral – lasting mere seconds or minutes. Another element adding to what is already a complex situation is security teams being tasked to secure operational technology (OT). According to the same Forrester study, 61 percent of Saudi organisations who had suffered a business-impacting cyber-attack in the last 12 months said these attacks involved their operational technology (OT) systems.

Security leaders must work with their business partners to determine what it is the business unit does, and which services and applications are critical to accomplishing core tasks. This intelligence informs the security team to focus protection efforts. This also clarifies who the asset owners

are should an incident arise, enabling infosec teams to respond more quickly in order to limit damage.

"BUSINESS-ALIGNED

SECURITY LEADERS CAN

CONFIDENTLY EVALUATE

THE REAL RISKS TO THE

CRITICAL ASSETS THAT

EFFECT ON THE BUSINESS."

HAVE THE GREATEST

Identify real versus theoretical risks

The next challenge is to prioritise from the tens of thousands of threats and vulnerabilities in existence which pose a real versus theoretical risk to the organisation. This determines how exposed the organisation is, how quickly vulnerabilities can be addressed and the cost to the business to mitigate the issue versus doing nothing.

Take action

When it comes to risk management, the businessaligned security leader is perfectly positioned at the intersection of technology and business to make an impact.

Understanding all critical processes and assets, from a broad enterprise risk perspective, makes it easier to secure the organisation.

In tandem, there are operational benefits from performing risk management exercises. What is identified will help the entire organisation understand how to prioritise resources both people and resources — to keep the business running, whatever happens.

The business aligned security leader

Business leaders need a clear picture of the risks faced. They also need to understand how that risk is evolving as they plan business strategies.

> Business-aligned security leaders can confidently evaluate the real risks to the critical assets that have the greatest effect on the business. They will report this risk in metrics the business understands -

customer churn. spoiled goods, etc. This provides an unambiguous, authoritative, answer when asked, "How secure, or at risk, are we?"





CHANGING THE GAME



CYBEREASON CEO AND CO-FOUNDER **LIOR DIV** SHARES THE COMPANY'S JOURNEY TO SUCCESS AND DISCUSSES HOW THEY ARE TRANSFORMING THE LANDSCAPE TO EMPOWER ENTERPRISES WIN THE CYBER WAR.

ounded in 2012 by three former members of an elite cybersecurity military unit, Cybereason offers innovations around endpoint protection, detection and response; next-generation antivirus; managed monitoring and IR services. Its flagship solution, the Cybereason Endpoint Detection and Response Platform, leverages Big Data, behaviour analytics and machine learning to uncover, in real-time, complex cyber-attacks designed to evade traditional defences.

At the time of the Cybereason's inception, many companies were

still at the early stages of their digital transformation journeys and investments were focused more on security rather than cybersecurity. This meant that while they have the technologies and solutions in place to secure their systems, they remain one step behind against threat actors and they lack the knowledge and capabilities to keep up with them, let alone stay ahead.

Lior Div, Cybereason's CEO and cofounder, together with his two other cofounders Yossi Naar and Yonatan Striem-Amit who are now the firm's Chief Visionary Officer and CTO respectively, recognised this gap in the market and sought to develop a game changing platform that will give enterprises an edge against cyber adversaries. "We realised that despite many companies excelling in their security ventures, hackers still have a significant advantage against enterprise security teams," explained Div. "Threat actors are constantly innovating and oftentimes an organisation is unaware that they are under attack until it's too late."

Driven by their military background, Div and his co-founders built Cybereason with an offensive mindset and with a comprehensive understanding of adversaries and their techniques, which were reflected in their security technology and service offerings.

"We wanted to be able to answer a simple question, 'Am I under attack?'," said Div. "So, we started building our flagship offering, the Cybereason



Endpoint Detection and Response platform, on the premise that most organisations have already been (or will be) breached.

"It took us more than two and a half years to develop and at the end of it we can say that we have come up with a technology that can easily identify whether an organisation is under attack or not at a given moment."

"AS A CYBERSECURITY BUSINESS, WE BELIEVE THAT OUR SUCCESS IS NOT ONLY ABOUT SELLING OUR TECHNOLOGY. IT IS ABOUT BUILDING A LONG-TERM PARTNERSHIP WITH OUR CUSTOMERS."

Currently, the Cybereason platform delivers a ratio of one analyst to 150,000 endpoints, compared with the industry benchmark of one analyst to 20,000 endpoints, making Cybereason the highest-performing EPP in the market today.

Div highlighted that their technology can bridge the gap between IT security and cybersecurity, which effectively protects an organisation against existing and even new types of attacks.

Headquartered in Boston, with three additional global offices in London, Tel Aviv and Tokyo, Cybereason has more than 600 people within its workforce and over 700 customers across the globe. The cybersecurity firm has also raised more than \$400 million in funding with Japan-based SoftBank



group among its main investors. The company now has a valuation of \$1 billion and was named a 'Forbes 2019 Next Billion-Dollar Startup.'

Earlier this year, Cybereason has launched its Middle East operations with Dubai as its base and regional IT security veteran Tarek Kuzbari at its helm.

Apart from having an operative mindset, Div also emphasised the company's 'glocal' approach as one of its key strategies for growth.

"As a global company with customers across more than 30 countries, we make sure that we hire the best local talents in each of the markets that we are in to grow our brand and deliver our technology and expertise," he said. "As a cybersecurity business, we believe that our success is not

only about selling our technology. It is about building a long-term partnership with our customers."

He added, "In order to do this, we need to have a good understanding of the different requirements that they have, recognising the challenges they face and even knowing their culture. This allows us to provide the support and protection they need in the same language they know both literally and figuratively."

But, perhaps, more than the company's innovative technologies and services, and impressive growth streak, another key factor that makes him proud of Cybereason is the dynamic and diverse culture within the organisation.

"We have come a long way since we started the company eight years ago, from three people we have now

grown multi-folds," said Div. "When we started this journey, I said to myself, we need to do this the right way from the beginning itself. So, we set up the business with five core values in mind. First, is we have to be daring, meaning we have to dare to win and fight against cyber-attacks in order to succeed. Second, is we have to be ever-evolving, this means that we have to progress with the landscape and evolve against hackers. The third value is to never give up because as we battle against these hackers we should continue to fight and fulfill our promise to protect our customers. Fourth is winning as one, meaning that everything that we do, we do together not just within the company but along with our customers and partners as well."



The final and, perhaps, the most important core value, according to Div, is the company's UbU (you be you) outlook.

UbU is an initiative that is focused on fostering diversity and inclusivity within the organisation.

"We believe that we can only solve some of the world's most complex technology challenges by unlocking the full talents of everyone within our organisation. UbU is about ensuring that our employees realise their fullest potential regardless of their age, race, religion and gender," he said.

Looking ahead, Cybereason aims to continue to be a key player in the multi-

billion-dollar endpoint security market by aggressively obtaining new customers, onboarding talents and finding new growth opportunities. The company envisions to be an icon in the cybersecurity space in the next few decades.

"Cybersecurity, or lack thereof, is a global problem. That's the reason why we're aggressively expanding all over the world," said Div.

According to Div, they want to address this problem by protecting what they call the triple Es – endpoint, enterprise and everything.

"We started by defending all endpoints and then we progressed to protect enterprises. And, ultimately, as things become more connected – from our phones, PCs, cloud, TV and cars – we aim to protect the 'big E', which is everything. Our vision is to become the company that can and will protect it all. At the end of the day, Cybereason's long-term mission is not just to protect endpoints but to end cyber-attacks." 1

"WE BELIEVE THAT WE CAN ONLY SOLVE SOME OF THE WORLD'S MOST COMPLEX TECHNOLOGY CHALLENGES BY UNLOCKING THE FULL TALENTS OF EVERYONE WITHIN OUR ORGANISATION."



Hikvision Temperature Screening Thermal Solutions

SAFER, FASTER, SMARTER



Contact-free



Multi-person detection





Thermographic Cameras

MinMoe Terminals

Metal Detector Door

DeepinMind NVRs

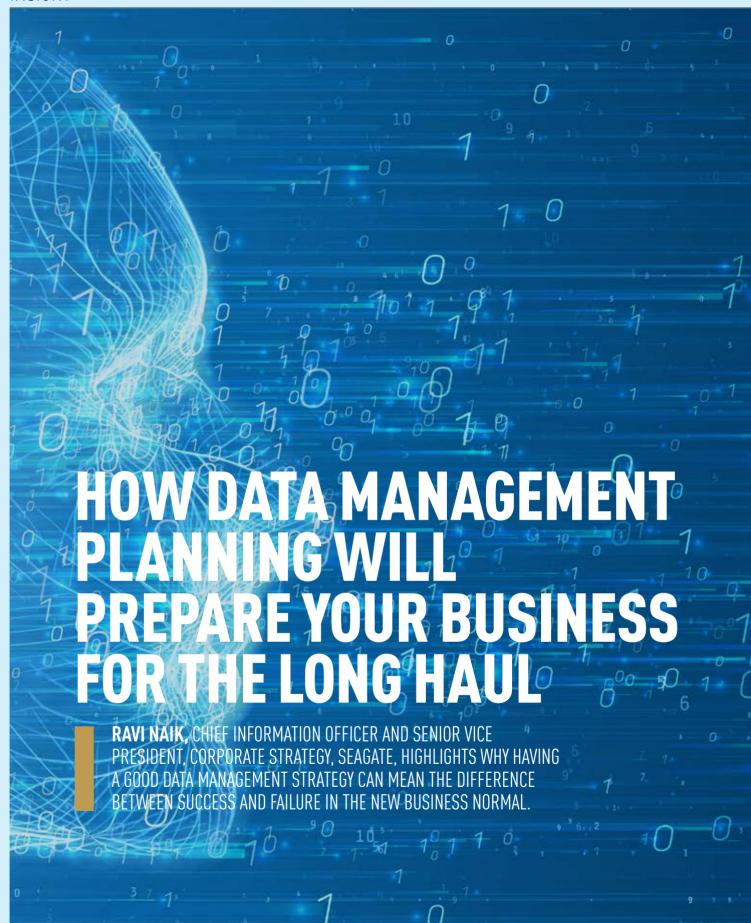




Temperature Screening Thermal Cameras

For more information, please scan the QR-Code to visit our Temperature Screening Thermal Solution page.





ockdown is easing but many of us continue to work from home. The longer this continues, the more we rely on data to do the legwork. One of the great successes during the crisis has been remote working technology. Whether through videoconferences or virtual team quizzes, we have been able to rely on technology to keep us online and working, as well as in touch with our colleagues.

Whether text communications, product usage patterns, or financial performance figures – data is vital to businesses. This means good data management – collecting, maintaining, and using data effectively – has never been more important.

Businesses must make it a top priority. Here are some best practices for any business looking to get control of their data to prepare for long-term remote working.

Smoothen data access and shore up connectivity

Making access to data as smooth as possible for employees should be fundamental to any data management plan. Any friction staff encounter when accessing data will be reflected in reduced productivity and increased costs. The easier data is to use, the more valuable it is.

Improving access to data can mean something as simple as standardising file names and making them less unwieldy. It can also mean upgrading your reporting system and giving employees better training on using it, reducing the chances of human error. And if you do not have a VPN, make implementing one a priority. VPNs provide safe pathways to vital files remotely while maintaining security protections other data management solutions might lack.

Quality over quantity

Having a large amount of business data means nothing if the data is of poor quality and cannot be used effectively. Yet too many businesses prioritise sheer volume of data collection over the quality of the data they're collecting. Duplicated records, wasted storage space, errors, unstandardised record formats – all are cardinal sins commonly found throughout businesses' data storage that make data less useful.

Ravi Naik, Seagate

"HAVING A LARGE
AMOUNT OF BUSINESS
DATA MEANS NOTHING
IF THE DATA IS OF POOR
QUALITY AND CANNOT
BE USED EFFECTIVELY."

And bad quality data can even actively harm a business if your analysis leads to poor decisions. For example, a business might cut a marketing campaign that data shows is underperforming – while in reality its impact is just not being recorded properly.

To help promote data hygiene, businesses should consider establishing a regular data audit to spot and remove bad data. Investing time and money in this area will pay off long term. With fewer errors and a more standardised format, data analytics will be more insightful – and therefore more valuable.

Review security, backup and recovery practices often

Remote working presents all kinds of security challenges. Firms have less oversight of employee activity, and shadow IT becomes an even greater risk with employees relying on the consumer apps they know when faced with a problem – rather than more unfamiliar enterprise-grade software.

Implementing and regularly reviewing your data backup and recovery contingency plans is just as important as overall security. Accidents happen:



whether through human or machine error, data corruptions and file losses are an inevitability of doing business.

A backup and recovery plan should make it clear how different types of data should be backed up, and a step-by-step account of how they are to be recovered. And do not forget about the human element – IT decision-makers should work with HR in ensuring best practices are upheld consistently.

Test your flexibility

Covid-19 forced many businesses to make radical changes to their IT at short notice. The middle of a crisis is a poor time to make such changes, but lockdown left no choice.

Looking ahead, the future is uncertain. We have not yet returned to normal, but we have at least grown more accustomed to the current situation. If there was ever a time to test your flexibility, now is the time to do it. Businesses should stress-test their systems, re-assess the effectiveness of their tools, and prepare for the unexpected. We may yet see a second wave, and there will inevitably be longerlasting economic and social consequences of lockdown. But with a robust data management plan, businesses will be well-placed to weather the storm.

A NEW WORLD OF THREATS

MIMECAST GENERAL MANAGER FOR MIDDLE EAST **WERNO GEVERS**SHARES THE LATEST FINDINGS OF THE MIMECAST STATE OF EMAIL
SECURITY REPORT, AND DELVES INTO WHY TODAY'S THREAT LANDSCAPE
CALLS FOR MORE PERVASIVE SECURITY STRATEGIES.

he ongoing COVID-19 pandemic has resulted in a tremendous shift in the way businesses operate. How has this impacted the cybersecurity landscape?

The global spread of the coronavirus has created many new opportunities for threat actors. We've seen in that since the first 100 hundred days since the virus began, overall threats activity has increased significantly rise by 33.5% which are focused largely on high volume, spamming and impersonation attacks. These tactics enable attackers to target a large number of potential victims with the least possible effort. We've seen that these attacks come at the time when an unprecedented combination of risk factors make people particularly vulnerable, I think that is illustrated by the fact that users are clicking on unsafe links as they seek for more information about the crisis. Over this period as well, we have witnessed that the number of clicks on blocked URLs has increased more than 751%, which is significant. As we continuously monitor these attacks, we've found that the latest coronavirus-related attacks are evolving to target government and businesses are also rising.

As companies transition to a remote workforce and the fact that click rates on these malicious links are rising are clear

indications of people letting their guard down as they become desperate to learn more information about the pandemic. I believe that the rise in unsafe clicks suggests that there is an urgent need for organisations to refresh awareness training for employees and to rethink security strategies.

According to Mimecast's latest
State of Email Security report, we
have witnessed an uptick in BEC,
impersonation fraud and email phishing
attacks during the first 100 days of
COVID-19. What have been the primary
drivers behind the increase of such
cyber threats, and can we expect this
trend to continue in the coming months?

I think the State of Email Security report is one of our most downloaded assets globally. Today it has become more vital as many employees are working from home and are using cloud tools to be productive.

This report is instrumental in enabling us to look after our customers.

OF UAE FIR TARGETED IMPERSO BEC

The report saw that cybercriminals are

refocusing their phishing impersonation and ransomware attacks from office networks to the cloud services to target those remote employees. We've also seen that the global pandemic is accelerating the cloud adoption immensely. We've seen a massive surge in the demand for software-as-a-service based collaboration solutions. However, many organisations found that they weren't equipped for remote working environments. This meant that employees who are working from home for the first time may not be sufficiently aware of the cyber threats and how to mitigate them. In fact, our research has found that employees from companies not using our security awareness training service, we're more than five times likely to click on malicious links than employees from companies that utilise the training.

In the UAE, the State of Email Security report showed that 70% of respondents reported encountering incidents of phishing, BEC and impersonation attacks due to the global pandemic. We've also seen that 17% of respondents stated phishing remained flat or increased for them. If you look at Saudi Arabia, 54% of the respondents reported the same or increasing phishing attacks at their organisations and 56% of the respondents had seen impersonation fraud increased or stayed the same.

In addition, our latest threat intelligence highlighted that one of the things is highly likely to occur during continued periods of

uncertainty is an increase in cyberattacks against vulnerable

> targets. At the end of the day, humans are the weakest links.

Therefore, the longer the pandemic remains a subject of significant concern across global communities, cyberattacks will continue to rise.

OF UAE FIRMS HAVE BEEN TARGETED BY PHISHING, IMPERSONATION AND BEC ATTACKS



How can organisations monitor and curb the disruptions caused by email-borne attacks? How can Mimecast help them address these challenges?

Historically, email security has been integrated with a secure gateway, which is a perimeter strategy to prevent malicious emails from making their way to corporate mailboxes. The changes in the threat landscape required such strategies to transform and extend beyond the traditional perimeter-oriented defence to a more pervasive one. This ensures that security is integrated into the company's overall systems and extends to protect applications such as Microsoft Office 365.

More than deploying secure gateways organisations need to understand that they need to manage human errors to mitigate the impact of internal email threats that could disrupt their business. Mimecast offers a wide range

of solutions including Email Security, Web Security, Brand Exploit Protect and DMARC, which have now all become incredibly important when it comes to protecting organisations as they navigate remote working environments. We also have a comprehensive backup and archiving solution, which help companies restore access to critical business data should there be any unplanned downtime.

Another key factor that they need to look into implementing robust security awareness training programmes. With today's a distributed workforce and an abundance of scams doing the rounds, the cost of human error escalates.

So, organisations need to take steps adequately to prepare them to spot these threats. Our research has shown that the most effective training needs to be short, fun, and engaging to help foster the security culture. Business leaders

"I BELIEVE THAT THE RISE IN UNSAFE CLICKS SUGGESTS THAT THERE IS AN URGENT NEED FOR ORGANISATIONS TO REFRESH AWARENESS TRAINING FOR EMPLOYEES AND TO RETHINK SECURITY STRATEGIES."

need to understand that security is every employee's responsibility and not just the security team's.

Ultimately, a pervasive security strategy requires a combination of robust email security and awareness training.

What can regional customers expect from Mimecast over the coming months?

We'll continue to build out our API platform with more integrations with leading brands. We believe that it is important for organisations to be able to invest in a service that could talk to their broader ecosystem. We have also recently acquired a company called MessageControl, a messaging security provider with solutions designed to help stop social engineering and human identity attacks with the use of machine learning and artificial intelligence. This powerful combination of Mimecast and MessageControl is engineered to provide customers using productivity apps, such as Office 365 or Google, which will give them stronger protection against the advanced phishing and impersonation attacks. It is also designed to prevent inadvertent loss of sensitive and confidential data while also serving as an additional sensor to further enrich threat intelligence.

For us as an organisation, we remain committed to keeping our customers safe and secure as the threat landscape evolves. In addition, we are going to continue evolving our services and platforms to ensure that we deliver the best protection to our customers. 1



inadequate incident response plans. They also became more aware that any misconfigurations in their systems can lead to sensitive information being exposed and vulnerable to threats such as DDoS attacks.

Over the past few months, we have also seen a big influx in cybercriminals taking advantage of the COVID-19 pandemic to scam consumers and launch targeted attacks. In most cases, people who are desperate for more information about the ongoing crisis are the ones that are falling prey to these types of attacks.

Today, to stay resilient, organisations need to have a better understanding of remote access systems and implement the necessary security measures.

What are the most prevalent cybersecurity challenges remote workforces are facing today?

As employees continue to work remotely, they face a range of challenges from phishing attempts to email fraud, poor technical infrastructure and inadequate cybersecurity measures from their own companies. So, if employees are expected to work at the same pace as before, they will require the latest technologies, robust security solutions and reliable network connections.

Another challenge brought by the sudden move to remote working is employees cutting security corners.

Oftentimes, this is caused by the lack of cybersecurity training within the workforce. However, in many cases, there are personnel who find security policies disruptive to their productivity, which results in them bypassing such regulations, putting the entire organisation at risk. In addition, because of the shift from the usual work setup, IT security teams are unable to quickly respond to the issues raised by remote workers and users.

I believe that in the coming months, we can expect cybercriminals to continue

exploiting these vulnerabilities and that is something that organisations and their security teams need to be prepared for.

What steps should organisations take to ensure that their workforce is practising good cyber hygiene while working remotely?

As a measure to stay secure amid the current landscape, I cannot stress enough how important it is to implement policies around strong password and access management for various endpoints and applications. End-users should also practice good cyber hygiene by ensuring that they keep their devices secure even when not in use. They also need to refrain from using corporate devices for personal use to reduce the risks of a breach. IT leaders should also look at implementing full-disk encryptions so in case an employee's device is misplaced they can rest assured that the company's data do not fall into wrong hands.

Another best practice they can follow is leveraging a Virtual Private Network (VPN), to ensure that the corporate network is secure as employees constantly access it remotely. It can prevent man-in-the-middle attacks since working from home means that all data is actually flowing into a public network.

A major challenge for enterprises has been maintaining business continuity while ensuring

cybersecurity. How is ESET helping organisations stay secure while remaining agile amid the 'new normal'?

Our top priority has always been to help our customers protect their systems and data. In line with this, during the early months of the pandemic, we did as much as we could in order to support businesses. For our existing customers, we offered a renewal extension for those that have licenses that are about to expire. We also offered a 90-day extended free trial on some of our products including

"IF EMPLOYEES ARE
EXPECTED TO WORK
AT THE SAME PACE AS
BEFORE, THEY WILL
REQUIRE THE LATEST
TECHNOLOGIES, ROBUST
SECURITY SOLUTIONS
AND RELIABLE NETWORK
CONNECTIONS."

the ESET Dynamic Threat Defence, a solution that utilises cloud-based sandboxing that helps detect new, neverbefore-seen types of threats. Additionally, we also extended trials for our ESET Secure Authentication solution, which enables companies to ensure seamless and secure access to their networks.

We also ran special promos for new customers to give them the opportunity to leverage and experience the benefits of our solutions amid these challenging times. Along with this, we also provided them with access to our technical teams to help them identify the best solutions to protect their business.

What can the market expect from ESET in the coming months?

Looking ahead, we believe that remote working models are here to stay. It is the new normal. So, our focus will be on remodelling our existing solutions to be more adaptive towards a home office for the business environment to help companies function in an efficient and secured way. We are also looking at launching new solutions that are focused on cloud setup and cloud utilisation later in the year.

Overall, we want our customers to know that we are here to help protect their organisations against cyber threats and help their workforce to work securely.

SPOTLIGHT: BRYAN SEELY

IN AN EXCLUSIVE INTERVIEW, SECURITY ADVISOR ME EDITOR ADELLE GERONIMO SPEAKS TO WORLD-FAMOUS CYBERSECURITY EXPERT, ETHICAL HACKER, AUTHOR AND EX-US MARINE **BRYAN SEELY** WHO REFLECTED ON HIS CAREER AND PERSONAL EXPERIENCES IN THE WORLD OF CYBERSECURITY.



n 2014, network engineer and ex-US Marine Bryan Seely made headlines when he was hailed a "hero" after he intercepted and recorded calls to the FBI and the Secret Service.

For years he has been trying to get Google's attention about the security weaknesses on the location listings added to Google Maps. When they didn't pay heed to his warnings, Seely took a big, bold step to get the tech giant to listen. He exploited a vulnerability in Google Maps' verification process and established fake contact information for the FBI and Secret Service by replacing the numbers on the listings with his own phone numbers. He then routed the incoming calls to the correct numbers and recorded the conversations.

Seeley eventually took the information – and recordings – to the Secret Service office in Seattle, where he was read his Miranda rights and put in an interrogation room. After a few hours of questioning, Seely was then allowed to leave and the Special Agent in charge praised him for bringing this major security flaw to light.

Since then, Seely has enjoyed a growing career in the world of white hat hacking. He started his own company called Seely Security. He was also personally recruited by business mogul Mark Cuban, appointed to McAfee Global Technologies' Hacker Advisory Board, and uncovered vulnerabilities in high visibility sites like LinkedIn.

During the sidelines of the recently held GISEC virtual conference, Seely candidly reflects on his career as an ethical hacker and cybersecurity advocate.

Can you tell me a bit about how you came about being an ethical hacker?

I've always been interested in computers. My sister was named Lisa after the Mac Lisa, one of the first Apple computers that were ever made. I think I had my first computer when I was two and a half years old. I've been on the computer ever since. I guess, I missed the day in school when boys learned how to talk to girls because I was probably on the computer.

I became more involved in hacking and cybersecurity 10 years ago and I took it more seriously in 2013. It's mostly because I find puzzles interesting. I find the challenges and finding stuff that other people don't see, very exciting. This led me to arguing with Google back and forth about the vulnerabilities that can be exploited on Google Maps to scam consumers. It was kind of a rampant problem. So, in my exchange with them, I demonstrated these issues in some funny ways and then in some serious ways that almost got me into a lot of trouble. I wiretapped the Secret Service and the FBI, which was not a good plan, but it worked out pretty well.

Since then, I have given Ted Talks about the whole incident, I worked with Mark Cuban and uncovered multiple problems high-profile flaws on LinkedIn. I also ended up working for John McAfee and went to Defcon with him. I've met some really cool people and worked with politicians and high profile individuals; the list goes on. Sometimes, I will get random calls from people saying they saw me on the news, and they want my help to hack an unfaithful spouse and all sorts of crazy stuff every single day. My life has definitely been an adventure.

It's been more than half a decade since you exposed the Google Maps scam, do you think that the company is doing enough to address this issue? What do you think needs to change?

Well, they had taken some action

but I don't think it's enough and it's definitely not perfect. The next step would have to be working with local governments to validate the content and to determine which business is legitimate or not. The governing bodies that grant licences to businesses should communicate with Google to identify the illegitimate businesses that are promoting themselves on Google's platforms to stop them from scamming consumers. Because ultimately online can be a dangerous place if there's no accountability.

Do you think black hat and nation-state hackers are morally corrupt?

That's a hard question. I think it would be better if no one was hacking anyone. But I don't think anyone would simply stop if one country just said, "Okay, we're not going to hack anybody, but leave us alone." That's not going to happen. So, I think this is something that we need to accept as part of the world we are living in. However, I don't believe that countries simply set out to sabotage another nation or cripple their infrastructure and harm civilians. I think not all of the important arguments or sensitive information are being presented to the public for us to understand. There may be situations where what they're doing is about preventing a hack that was first directed at them. I don't think it comes from a

"I GOT MORE INTO HACKING AND CYBERSECURITY 10 YEARS AGO AND I TOOK IT MORE SERIOUSLY IN 2013. IT'S MOSTLY BECAUSE I FIND PUZZLES INTERESTING. I FIND THE CHALLENGES AND FINDING STUFF THAT OTHER PEOPLE DON'T SEE, VERY EXCITING."

place where they intentionally want to destroy other people's way of life.

Has anyone from Russia or China ever tried to recruit you to be a hacker for them?

No, I don't think so – no one with a Russian or Chinese accent. I've always worked on the ethical side of things. I've worked for companies that had very, very secret information such as patent trademarks and I would never sell it for any price because it's not the right thing to do. I wouldn't want to go to sleep at night knowing I have done something bad.

What has been the most memorable or challenging case or project that you have handled?

I think it was more of a personal case. Four and a half years ago my stepdaughter became a victim of human trafficking. She went missing and for months I was looking for her. I found her before the FBI did and the agent in charge said that he's been handling investigations like that for 17 years, and they've never seen a parent find their child before the authorities do. That incident was very emotionally trying for me. I had to stop a lot of projects to recover from what happened.

What can we expect from you in the coming months?

I am working on a new book and am writing some new speeches on cybersecurity and other topics. I recently guested on a podcast called "Amplified" with Terry Tateossian, where I discussed the incident with my stepdaughter. I think it's time to educate and talk to people about these situations because I think it will help. This issue is part of the new realities that parents have to cope with. They need to be aware and understand that the Internet is now becoming even more dangerous for kids. 1



mart security is advancing rapidly across the UAE. As AI and 4K rise in adoption on smart video cameras, these higher video resolutions are driving the demand for more data to be stored on-camera.

Complex, extensive camera networks already require a large amount of data storage, particularly if there is 24/7 monitoring from smart videoenabled devices. With 4K-compliant cameras projected to make up over 24% of all network cameras shipped by 2023 – there is a fast-growing desire for reliable storage on-board security

cameras. The question for businesses is: do they look to break up their existing smart video network, by separating and compartmentalising cameras to handle data requirements, or do they increase its storage capabilities?

As some people begin to venture out and return to work following initial COVID-19 measures, we are seeing demand increase for thermal imaging technology. New technology like this combined with more always-on systems being rolled out, mean organisations will need to carefully consider their smart video strategy. Previously, companies have preferred public cloud adoption. However, we are now seeing data processed at the edge, rather than in the cloud. One main reason for this change: latency.

EDGE COMPUTING AND SMART SECURITY

Previously, companies have preferred public cloud adoption. However, we're now seeing data processed at the edge, rather than in the cloud. One main reason for this change: latency.

Latency is an important consideration when trying to carry out real-time pattern recognition. It's very difficult for cameras to process data – 4K surveillance video recorded 24/7 – if it has to go back to a centralised data centre hundreds of miles away. This data analysis needs to happen quickly in order to be timely and applicable to dynamic situations, such as public safety. By storing relevant data at the edge, Al inferencing can happen much faster. Doing so can lead to safer





Barber Brinkman, Western Digital

"BY STORING RELEVANT DATA AT THE EDGE, AI INFERENCING CAN HAPPEN MUCH FASTER."



software systems fail. In the event of this, it is important to establish a failover process to ensure continued operation or restore data after a failure, including everything from traffic control to sensors to camera feeds and more.

Consider the example of a hospital with dozens or even over a hundred cameras connected to a centralised recorder via IP. If the Ethernet goes down, no video can be captured. Such an event could pose a serious threat to safety and security. For this reason, microSDTM cards are used in cameras to enable continuous recording. Software tools – powered by AI – can then "patch" missing data streams with the content captured on the card to ensure the video stream can be viewed chronologically with no content gaps.

communities, more effective operations, and smarter infrastructure.

WD Purple Surveillance Hard drives have been engineered specifically for the extreme demands of high temperature, 24/7 surveillance systems. Built for always-on, high-definition security systems, WD Purple drives are designed to support deep learning analytics in Al capable NVRs, and feature an enhanced workload rating of up to 360TB/yr.

ALWAYS-ON CONNECTIVITY

Whether designing solutions that have limited connectivity or ultra-fast 5G capabilities, most smart security solutions need to operate 24/7, regardless of their environment. Yet, on occasion, the underlying hardware and

THERMAL IMAGING

Health and safety are the number one priority for all organisations as people return to work and public spaces across the UAE. Some organisations are deploying thermal imaging to help screen individuals for symptoms as they return. Organisations that operate with warehouses, depots and assembly lines will traditionally have large amounts of cameras located outside of the entrance. With thermal imaging smart video in place, these cameras can now serve a

dual purpose as a screening device. The thermal imaging technology is capable of detecting elevated body temperatures, with 10-25 workers being scanned in one shot, from one camera – making it an efficient and accurate process. This way, staff can use the information to help identify people who may need further screening, testing, and/or isolation before returning to work.

While this may not increase data storage requirements, it can change your retention policies and practices.

Smart security today is about utilising Al and edge computing, to deliver an always-on, high-resolution video provision that can help keep people safe 24/7. These trends increase the demands and importance of monitoring, which means prioritising the supporting data infrastructure, including the ability to proactively manage the infrastructure to help ensure reliable operation.

Companies in the UAE need to make sure they have considered all the storage and policy challenges as part of their smart security strategy and Western Digital can help. Western Digital provides an unmatched portfolio of products, including WD Purple™ HDDs and microSD cards, to capture video for real-time analysis and actionable insights. Find out more at https://www.westerndigital.com/solutions/surveillance. ▮



019 saw a significant rise in ransomware attacks on public sector targets. Specifically, these attacks have been targeting local government departments. With this insight the Home Office has published a series of recommendations for cybersecurity teams to utilise on relevant threats. These guides cover threat intelligence, threat hunting and digital risk and intelligence, deriving from a series of conversations with stakeholders in government and industry around their current capabilities. One of these guides highlights a recommendation to use a security operation centre to reduce risk, along with investing in the development of people involved in the effort, and ensuring essential data is visible. But, as the rate

of attack is increasing and, unfortunately, government cyber defences are still struggling to keep pace, it is important to explore more thoroughly the key challenges being faced.

RESOURCES

One of the most significant risk areas identified by the public sector generally is internal resources – people, technology and funding. These resource limitations mean that government departments do not have the capability to combat the current threat environment.

Unfortunately, the prospect of significant hiring to augment this resource shortage is bleak, given a widening skills gap issue. Government IT and security teams are doing their best to establish situational awareness by combining raw threat



Steve Rivers, ThreatQuotient

"ONE OF THE MOST SIGNIFICANT RISK AREAS IDENTIFIED BY THE PUBLIC SECTOR GENERALLY IS INTERNAL RESOURCES – PEOPLE, TECHNOLOGY AND FUNDING."

feeds with existing security information and event management (SIEM) and log management tools. However, this approach fails to achieve this objective and ultimately drives up alert fatigue for an already overwhelmed staff. Eliminating alert fatigue and accelerating situational awareness requires prioritised, contextually relevant, real-time threat intelligence that seamlessly integrates with existing tools and practices. A threat intelligence platform (TIP) facilitates this integration. The result is the optimisation of limited resources.

SENSITIVITY TO BREACH

Local councils and government face the continual challenge of balancing access and transparency against protecting sensitive information. Doing this requires a level of openness that makes it impossible to prevent all intrusions. Complicating matters, most of the emphasis to date for government security has been on preventive tools, techniques and procedures. This is where government departments and local councils must shift their focus beyond prevention to include detection, response and recovery. Actionable threat intelligence, integrated with existing preventive tools via a TIP, is the best means to quickly detect, respond and recover from a malicious intrusion.

THREAT LANDSCAPE

The public sector is facing an everexpanding threat landscape driven by two factors. First, the abundance of legacy IT provides a broad target for malicious actors due to the persistence of unpatched, unprotected and even unsupported operating systems and applications. Second, the public sector is moving to the cloud and adopting mobile and Internet of Things (IoT) devices at an accelerating rate. These technologies, whilst critical to delivering new levels of government service and constituent responsiveness, significantly increase the attack surface. Maintaining current visibility into the entire infrastructure and continually re-evaluating and reprioritising threat intelligence helps government agencies protect an expanding digital environment against a growing threat landscape.

ADDRESSING THE SECTOR CHALLENGE

This is where situational awareness and response is key to the public sector in addressing the challenge. The first action necessary to address cybersecurity risk is to "increase cybersecurity threat awareness". A robust threat intelligence platform gives government agencies the prioritisation, contextual awareness and real-time insight necessary to accelerate detection, collaborate on response, accelerate recovery and achieve a rapid response. Utilising fully integrated platforms with already-in-place threat feeds and SIEM systems ensures that the sector is able to maximise existing resources such as staff and technology. As the threat environment continues to intensify, prioritising protection against ransomware and other disruptive cyberattacks will be critical to keeping public sector services operational. 🛚

UNLOCKING THE VALUE OF THREAT INTELLIGENCE

WITH INCREASING COMPLEXITIES AROUND CYBERSECURITY, THE NEED FOR THREAT INTELLIGENCE IS BECOMING MORE APPARENT. **AHMED ALI,** VP OF SALES FOR EMEA AT CYWARE, EXPLAINS HOW THE COMPANY'S INNOVATIVE OFFERINGS CAN ENABLE ORGANISATIONS TO LEVERAGE THE STRATEGIC VALUE OF THREAT INTELLIGENCE

oday's ever-evolving threat
landscape and growing
sophistication of cyber-attacks
make defending organisations
a Herculean feat. That's why
to gain an edge against threat actors,
IT leaders need to be able to predict
future attacks so they can prioritise their
responses and accelerate the decisionmaking process as well as response time,
providing better security altogether. To do
this, threat intelligence is paramount.

With data at its core, threat intelligence provides context such as who is orchestrating the attack, what their motives are and what indicators of compromise should you look for, which help organisations make informed decisions about their security.

The Middle East has witnessed a significant increase in threat intelligence solutions over the past year. In the UAE, a recent industry study highlighted that 69 percent of businesses view threat

intelligence as extremely important for their security strategies. A key driving factor behind this is the growing demand from organisations to be at the leading edge of security and the need to incorporate threat intelligence for more effective security operations.

Seeing this strong demand and opportunity, threat intelligence and cyber fusion products provider Cyware has recently entered the Middle East market and signed a distribution agreement with regional VAD Exclusive Networks.

Headquartered in New York, Cyware develops innovative solutions that deliver capabilities for strategic and tactical threat intelligence sharing, cyber fusion, security orchestration and automation, and incident response. The company also has a DevHub in Bangalore and an office in Mumbai. Over the last year, the company has seen tremendous growth, adding new customers across the globe and expanding its team and operations in nearly every department.

The company extended its footprint into the region in late 2019 with its operations based in Dubai. At the helm of its regional business is its VP of Sales for EMEA Ahmed Ali.

"Threat intelligence is vital in fortifying the defences of the security technology stack at any organisation," he says.
"Knowing what to defend against and how best to prepare for and prevent potential threats are they key benefits of threat intelligence. We have designed our threat intelligence platform solutions to make it as easy as possible to leverage automation and operationalise intelligence for a faster, smarter defence."

The use of threat intelligence provides numerous benefits in making security operations more proactive and understanding threat actor behaviour more effectively. When it comes to detecting and analysing threats at an early stage, tactical threat intelligence plays a central role by illuminating a

threat actor's tactics, techniques, and procedures (TTPs). Cyware's solutions make secure collaboration, cyber resiliency, and enhanced threat visibility a reality for organisations, sharing communities (ISAC/ISAO), MSSPs, and government agencies.

"There are four main tasks
that are vital to a security team's
role – prevent, predict, defend
and respond," explains Ali.
"Threat intelligence can help
organisations predict behaviours,
analyse them and then apply
those analyses into their prevention
measures. This will ultimately help them
bolster their defences and allow them to
better respond to threats."

As the cybersecurity industry continues to evolve, conventional approaches to defending an organisation's assets and networks against advanced threats are no longer sufficient. Combatting these complex threats pushes security teams to adopt a wide variety of security products and solutions, which results in the creation of huge volumes of threat information in different formats. This makes analysing, correlating and prioritising this information a tremendous challenge for security teams to effectively triage and respond to critical incidents. To help address this challenge, Cyware designed its Cyber Fusion Center.

"The Cyware Cyber Fusion Center offers SOAR and more. It unifies several security functions such as threat intelligence, vulnerability assessment and incident response among others into a single, connected platform. It enables organisations to increase the speed and accuracy of their operations while reducing costs and risk of analyst burn out," says Ali.

He adds, "Just like other SOAR platforms, it provides advanced orchestration and automation to stay ahead of increasingly sophisticated cyber

Ahmed Ali, Cyware

"WE HAVE DESIGNED
OUR THREAT
INTELLIGENCE
PLATFORM SOLUTIONS
TO MAKE IT AS EASY AS
POSSIBLE TO LEVERAGE
AUTOMATION AND OPERATIONALISE
INTELLIGENCE FOR A FASTER,
SMARTER DEFENCE."

threats. But what we have done differently is we developed a feature called 'connect-the-dots'. Now, what this feature does is once an organisation integrates Cyber Fusion into their security stack, it fetches data from multiple endpoints. It sifts through huge volumes of cyber incidents with varying information and coalesces them. It then leverages the platform's orchestration capabilities and fuses all the threat data from existing security tools to deliver the optimal response to these incidents."

Speaking about the firm's partnership with Exclusive Networks, Ali says that the VAD's robust vendor portfolio and vast channel network make them the right partner for Cyware in the region. "Exclusive Networks has a strong reputation as a distributor of IT and cybersecurity products. Prior to signing them on as our VAD for the region, they did their due diligence to ensure that we complement their current portfolio and presented us with a clear strategy on how they can further fuel our growth. With localised teams and a great technical

knowledge, we see them as an extension of our global team."

In the coming months, Ali says that they aim to continue to spread awareness about their capabilities and offerings in the region. "Just like every company across the globe, the COVID-19 pandemic has slowed down some of our go-to-market strategies. However, we took the last few months as an opportunity to enhance our marketing and awareness plans."

Moreover, the company also endeavours to further enable organisations across both public and private sectors to leverage threat intelligence to collaborate and develop advanced defences against today's cyber threats. "Cyware's growth is only just beginning. We've designed all our products to help teams build stronger and more resilient defences. More and more organisations are recognising this and are adopting our technology. The coming months will bring further success, growth, and increased product innovations," he says. "L



he Middle East region is known for its propensity to adapt. The past 12 years have doled out two global economic crises — 2008's Great Recession and the economic turmoil caused by COVID-19. It was here, in our region, that some of the world's greatest innovations occurred, as enterprises, public and private, found ways to do more with less. This was made possible because of cloud-computing ecosystems.

The latest changes have been so jarring that we have begun to casually throw around the phrase "new normal". And not without reason. Pure onpremises environments were rapidly becoming a thing of the past before the pandemic, not least because of the lure of cloud as a platform for cost efficiency and operational agility. The rising popularity

of remote working now guarantees that our future workspaces will be hybrid: New. Normal.

This presents many problems for security professionals — an eclectic carnival of devices; a vast attack surface; a lack of control over all of it; and, of course, rising expectations. Under such pressure, it would be tempting to take it one day at a time, procuring different components of a security solution in separate rollouts: endpoint protection, network monitoring, cloud security, container security, and so on. This approach, unfortunately, leads to an uneven threat posture — a multi-vendor tapestry plaqued by false positives and overworked human resources. In the hybrid-workplace future that is to come, we will need to do better.

The unified response

Let us take a step back and imagine what tools we can leverage to gain a properly filtered view of our technology environment that automates the mundane and alerts our security team only to genuine "activities" of interest. Let us consider what is required to ensure a holistic solution that does not cost us prohibitive sums while diverting resources from more innovative pursuits.

A unified cloud-based response fulfils all these ambitions and more. We will all soon have at least one foot in the cloud. And when it comes to security, the massive compute power extant within such environments is ideal when trying to deliver real-time information on everything from suspicious network processes to the upgrade status of apps



Hadi Jaafarawi. Qualvs

"A UNIFIED CLOUD-BASED
RESPONSE TO CYBERSECURITY
MEANS THAT ORGANISATIONS
CAN STOP SCRAMBLING AND
START WINNING, AND NOT JUST
AGAINST CYBER-ATTACKERS."

on the endpoints. Low latency is all important in delivering such capabilities, and the most practical and obvious place to find this responsiveness is in the cloud.

Real-time visibility ensures that you can manage the complexity of an environment where attacks can come from anywhere (a multi-vector response). In a world where the endpoint has become the new perimeter, users are now an even weaker link than before. A careless click or a thoughtless swipe and you may be dealing with a showstopping data exfiltration.

Weeding the garden

But you just as commonly may be dealing with a dismissible relic — an old penetration method fruitlessly seeking to exploit a long-patched software vulnerability. Your problem, if you run a

patchwork of vendor solutions, is that you cannot tell the difference. But with a unified, cloud-based threat assessment, your cloud "brain" has already decided your response, presenting a high-level view (with granular drilldown options) only of those risks classified as both new and potentially hazardous. This saves your tech team hours of combing disparate dashboards, reports and data logs trying to figure out if, and when, they should act.

Vulnerability management is handled similarly in such unified solutions. Not every vulnerability requires direct and time-consuming action. By maintaining a robust asset registry, the cloud brain can keep tabs on what critical upgrades are required on which machines, and very often apply them without the need for manual intervention. Yet more time is saved. And vulnerability management, detection and response (VMDR), endpoint detection and response (EDR) and network security are all bundled within the same solution, so policies can be set by security teams that are unified with those of other technology teams, and allow an organisation-wide stand against bad actors that recognises and accommodates all of your business' goals.

Freeing up responders

When all points of defence are coordinated in such a tightly unified model,
response capabilities are consequently
sharpened. Instantaneous action now
becomes possible. The latest critical
patches and the small-time digital
pests have already been taken care
of by automated processes. So, when
something with a potentially high risk is
found, trained professionals — whether inhouse or part of a managed service — are
available to act. And because of the bigdata capabilities of the cloud brain, actions
that are taken are targeted and effective.

In a changing world, we can ill-afford to scramble about learning new tricks. And yet, that is all that bad actors ever do. A unified cloud-based response to cybersecurity means that organisations can stop scrambling and start winning, and not just against cyber-attackers. Because once you can count yourself safe from the cyber-villain, you can finally devote your energy to enhancing customer service, partner engagement, operational efficiency and all the things that help you differentiate yourself in your operating market.

So much becomes possible when you have taken a unified threat posture.

NAVIGATING THE SECURITY LANDSCAPE IN THE NEW NORMAL

CHARBEL KHNEISSER, REGIONAL
PRESALES DIRECTOR, MENA, RIVERBED,
DISCUSSES WHY ORGANISATIONS NEED TO
NOT ONLY THINK ABOUT HOW EMPLOYEES CAN
SUCCESSFULLY COLLABORATE BUT ALSO HOW
THEY CAN SAFELY DO SO AS THEY ADJUST TO
THE 'NEW NORMAI' OF REMOTE WORKING

his mass shift to remote working in the wake of COVID-19 has had an enormous impact on the complexity of the security landscape. Traditionally, trust in business is established through face-toface interaction. However, when working from home and relying on collaboration tools, employees must now trust that the individuals they are dealing with are who they say they are without a robust way to validate identity. This, in addition to security steps being skipped such as consistently using a VPN as businesses prioritise uninterrupted workflows for employees, has drastically increased the attack surface for hackers and left businesses vulnerable.

As the landscape shifts, it is paramount that businesses evolve at the same pace and revise their security measures accordingly.

ESTABLISHING A NEW FORM OF TRUST

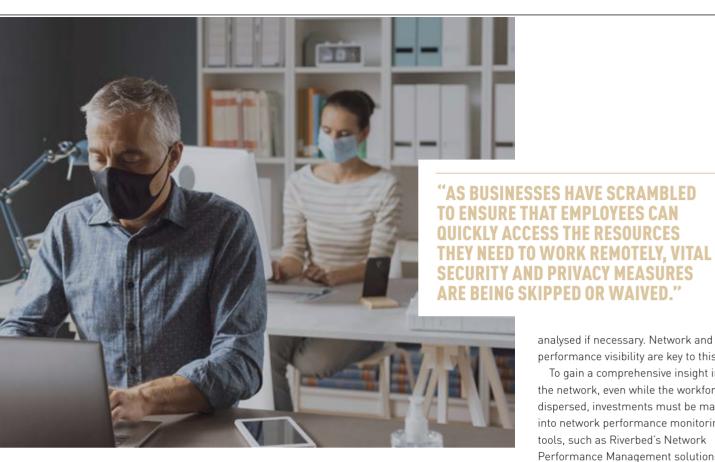
Collaboration

tools have been vital in ensuring that businesses maintain efficient operations during lockdown. However, they have not come without their security risks, including unauthorised visitors hijacking company meetings. As such, these tools have raised new complexities for the security landscape, and it is now vital that employees need to take a different approach to trust when using them. Within a typical office environment, employees primarily establish the authenticity of one another through a face-to-face chain-of-trust principle.

When working remotely, and relying solely on collaboration tools, traditional

security 'on-boarding' falls apart and it becomes more difficult to validate peers. This has proven only too true when using video conferencing tools, some of which have a notable lack of end-to-end encryption and secure passwords. Compounding this, many meeting organisers are not aware of important security features, such as meeting passwords. As such, cybercriminals are easily able to bypass the authentication process, putting companies at risk of hackers eavesdropping on confidential business calls. This not only leaves





a company's intellectual property vulnerable, but it enables the attacker to obtain information which can be used to impersonate employees and carry out spear phishing campaigns.

As organisations adjust to the 'new normal' of remote working, they need to not only think about how employees can successfully collaborate, but how they can do so safely. It is therefore crucial that businesses responsibly select the tools they choose - opting for those that offer true end-to-end encryption. This means tools that encrypt and decrypt communication at the sender-receiver level, rather than at the provider's server. In addition, they must educate employees on how to safely use these tools and the security risks if used incorrectly.

SKIPPING OUT ON SECURITY

As businesses have scrambled to ensure that employees can quickly access the resources they need to work remotely, vital security and privacy measures are being skipped or waived. This issue is

compounded by employees moving off the company network and increasingly using personal devices for work purposes at home. As a result, employers are losing visibility over employees' activity and their network. Without this cohesive visibility, IT teams are unable to troubleshoot problems, including security threats, as efficiently or effectively.

In order to avoid these issues, and ultimately ensure better security, it is crucial that businesses inform their employees of the importance of using the company approved VPN and their business devices.

ENSURING NETWORK VISIBILITY BEYOND THE OFFICE

It is now much harder for businesses to assess what is normal traffic on the network and separate the good from the bad. After all, traffic patterns are evolving faster than ever before. Businesses must adapt to this change and understand that in order to identify the signs of a security breach, they need to meticulously log information that can be forensically

analysed if necessary. Network and performance visibility are key to this.

To gain a comprehensive insight into the network, even while the workforce is dispersed, investments must be made into network performance monitoring tools, such as Riverbed's Network Performance Management solutions. These provide complete end-to-end visibility over the network and will forensically record the data to give IT teams different telemetry from multiple angles of the network.

EDUCATION, TECHNOLOGICAL INVESTMENT, AND TRUST KEY TO SECURE REMOTE WORKING

It is clear that remote working is here to stay. Even after the lockdown restrictions have lifted, the number of employees that will continue to work remotely either on a permanent or semi-permanent basis is likely to be high. As such, businesses must embrace long-term solutions now to ensure their employees are able to work securely and effectively from home. This means investing in solutions that provide comprehensive visibility into the network performance, educating the employees on safe remote working practices, and balancing this with employer-employee trust. Failure to make these adjustments will mean businesses' leaving themselves open to security attacks that could have damaging consequences for any company. 🙎



SEAGATE SKYHAWK AI

RELIABLE, POWERFUL AND INNOVATIVE – WE GIVE OUR TAKE AS TO WHY THESE THREE FACTORS MAKE SEAGATE SKYHAWK AI HDDs THE PERFECT ANSWER TO YOUR VIDEO SURVEILLANCE STORAGE NEEDS.

rtificial intelligence (AI) is becoming more and more prevalent across multiple fields. AI presents a plethora of benefits whether it be for eradicating time-consuming,

be for eradicating time-consuming, monotonous tasks; enhancing operational efficiencies and boosting customer experiences. From a smart surveillance standpoint, AI opens the door for intelligent real-time video analysis that will enable organisations to optimise ultra-high-resolution video as proactive security asset rather than a reactive, post-incident investigation tool.

However, these AI-enabled surveillance cameras generate bigger volumes of data, which require robust video storage drives that can support both AI and video workloads.

Seagate, through its line of SkyHawk Al purpose-build hard disk drives (HDD), seeks to address this growing demand for Al-powered video surveillance solutions.

The SkyHawk AI is a 3.5-inch HDD is available in 8TB, 10TB, 12TB, 14TB

and 16TB capacities. The device's body showcases the logos of both SkyHawk and Seagate, its capacity and a QR code that brings you to the drive's page on the company's official website.

The 16TB version, which is the highest one in the series, features a SATA III 6Gbps interface and a 256MB DRAM cache. It can store up to 10,000 hours of HD videos, and is capable of supporting up to 64 HD video streams and 32 AI streams. It has an average power draw of 6.71 watts when in use and 5 watts when idle.

At the core of the SkyHawk Al drives is Seagate's unique ImagePerfect Al firmware, which has been designed with an intelligent algorithm that reduces data errors, allows for perfect images to be stored without pixelisation, and prevents critical frame loss during multiple stream recordings. It also allows the HDDs can quickly wake up from idle and resume work.

In addition, ImagePerfect AI sports a special caching algorithm that allows low latency and reliable read performance to quickly locate and deliver video images and footage analysis. This feature, according to Seagate, enables on-the-edge decision making, eliminating the

latency of exchanging cloud-based data and processing.

SkyHawk Al drives have been designed to meet the growing demands for heavy-duty surveillance workloads, including the tasks of real-time video recording in complex video analytics-driven environments. The devices in the series are capable of supporting a workload of 550TB per year and boast the capacity for three times the workload of standard surveillance drives.

Furthermore, the AI-enabled HDDs are equipped with the SkyHawk Health Management software and optional Rescue Data Recovery services.
SkyHawk Health actively monitors and analyses drive health, empowering users to prevent, intervene and recover from potential anomalies.

Overall, the SkyHawk AI drives are perfect for delivering top storage performance while offering low power consumption. It is designed for longevity and is the ideal choice for any security and business team. If you're in the market for a reliable, powerful and innovative AI-powered HDD for your NVR and surveillance needs, we highly recommend the Seagate SkyHawk AI drives. 1

Clear access policy

ebrong passwords

Employees training

Secure networks

Latest Windows update

enswitoe eunivitaA

GETTING THE BEST VALUE OUT OF SECURITY ASSESSMENTS

BOJAN ZDRNJA, SANS CERTIFIED INSTRUCTOR AND CTO, INFIGO IS, DISCUSSES HOW ORGANISATIONS CAN CHOOSE THE RIGHT SECURITY ASSESSMENTS TO MAXIMISE THEIR SECURITY INVESTMENTS

here are many aspects to managing vulnerabilities in today's complex IT environments.

Performing security assessments is a popular way of identifying existing vulnerabilities, which then allows for proper mitigation. In this article we look at the differences between vulnerability scanning, penetration testing and red teaming, three security assessments that are popular, but that should be performed with care, in order to achieve best results.

Deciding which security assessment to perform depends a lot on an organisation's security maturity level, and the best results will be achieved by performing them exactly in the order listed – let's see why.

Vulnerability scanning (assessments) is something that every organisation should be doing on a regular basis. This is the first, and the most basic activity in managing vulnerabilities: the goal of a vulnerability scanner is to find low-hanging fruit and known vulnerabilities or misconfigurations. Vulnerability scanners will do a great job of enumerating installed

patches, finding default accounts and misconfigurations. Modern scanners can also authenticate against target systems (log in), which will allow them to list installed patches and correlate such information with actively obtained data from a scan, thereby reducing false positive reports.

It is recommended that vulnerability scanning is performed regularly in every organisation, preferably with internal tools. The most popular network vulnerability scanners are Rapid7 Nexpose, Tenable Nessus and Qualys. Just keep in mind that these should be used for network scanning, while other, more specialised tools exist for application level scanning (i.e. for web applications).

Penetration testing should be the next step. When deciding on a penetration test, scoping is very important: the goal of a penetration test is to find all (or at least, as many as possible) of the vulnerabilities in the target scope. The target scope can be a set of IP addresses or networks (when we talk about a network penetration test), a web application, web services and so on.

Since a penetration tester is normally limited in time (typically penetration tests last between 5-15 working days), it's obvious that the whole process should be as efficient as possible. This means that the scope should be as clearly defined as possible, and that any potential obstacles should be removed. For example, if you are testing a mobile application, it would be beneficial to provide a build without obfuscation for your penetration tester: we know what obfuscation can be circumvented and by providing such a build, the penetration tester will not waste time on deobfuscation, but on finding vulnerabilities.

Additionally, a penetration test will also test for vulnerabilities that a vulnerability scanner cannot find – for example, logic vulnerabilities. Business logic vulnerabilities are almost impossible for a vulnerability scanner to identify (at least for today's tools), and they can be devastating. A good example is, if you are a bank and have an Internet banking web

application; an attacker logs in and tries to create a transaction of -100 EUR, resulting in the payer receiving the funds instead of a payee. Or, another very common category of vulnerabilities is Direct Object Reference (DOR), when attackers try to access objects (for example, transaction records) belonging to arbitrary users by modifying object references. Since object references are typically just numbers (IDS),

"THE MAIN DIFFERENCE
BETWEEN A RED
TEAM EXERCISE AND A
PENETRATION TEST IS
THAT WITH A RED TEAM
EXERCISE THERE IS ONE
ULTIMATE GOAL, WHILE A
PENETRATION TEST AIMS TO
FIND ALL VULNERABILITIES
IN THE DEFINED SCOPE."

modification is easy, yet many scanners will miss such vulnerabilities since they do not understand the context i.e. the fact that by changing an ID and retrieving someone else's transaction record means we have found a critical vulnerability.

The result of a penetration test is a report that should detail all identified vulnerabilities, with recommendations on how to fix them. All listed vulnerabilities should be verified by the penetration tester – there should be no false positives there!

It is now clear that penetration tests require a lot of manual work – that's why they take quite a long time and are typically more expensive than a vulnerability assessment.

Finally, a red team exercise is the ultimate test of any organisation's defences. In a red team exercise, the attackers are given a final goal and they can typically use any means they want to achieve their goal. This might include writing new exploits, using social engineering, moving laterally and so on.

The main difference between a red team exercise and a penetration test is that with a red team exercise there is one ultimate



goal, while a penetration test aims to find all vulnerabilities in the defined scope. A red team exercise might miss some vulnerabilities and never report them, but it will show you how you stand against a real attacker. Quite often a red team exercise is a good test of an organisation's blue team – it will show how good they are in detecting attacks and potentially preventing them while they are happening.

Although the above is the ideal process for managing vulnerabilities within an organization, ultimately, deciding which security assessment to select also depends on the maturity level of the organisation. If, for example, the target organisation is not regularly patching its servers, there is no point in doing a penetration test or a red team exercise as even the basic security hygiene is lacking. This must first be addressed. It is only after low-hanging fruit has been taken care of, that a more sophisticated security assessment should be performed.

Likewise, if an organisation is releasing a new application, for example, then a penetration test might be more suitable since the goal will be to find all the vulnerabilities in the new application. And, if you have already tested the majority of your services, and have a trained blue team, a red team exercise will help show how prepared the organisation is against a real-world attack.

HOW ORGANISATIONS CAN ENSURE A SMOOTH TRANSITION BACK TO THE OFFICE

BY ARA ARAKELIAN, HR MANAGER FOR META, KASPERSKY

t is true when people say that the world will never be the same again after the COVID-19 pandemic. This situation has showed how vulnerable we are and made us reconsider our values, as well as review our habits and attitude towards many things, with the first being work.

Almost the whole world has switched to the remote work, which has never been done before and has significantly changed people's interpretation of their daily work routines. A common stereotype that is seen in many cultures that you can only work effectively by being in office has been broken. At the same time, people are wanting to go back to their offices as they feel the need for social interaction, which is of course the basis of every relationship.

While some countries have already started to ease self-isolation restrictions, businesses face an important question of being able to transition work back to the office. For instance, how can they make sure it safe as well as comfortable for employees? There are two essential points organisations need to consider: the human side of the question and the organisational one.

GOING BACK TO (NEW) NORMAL

As many countries relax the quarantine measures, businesses are starting to reopen, and more people will be coming back to offices in the coming months. We have already seen that many people at Kaspersky are eager to come back to the office, to finally see their colleagues and get back to their normal lives. However, while the coronavirus is still with us, the question

around employees' safety goes first. In fact, we will all have to find the right balance between our desire to go back to our normal daily routines and feeling safe. At Kaspersky. we regularly run surveys to understand the emotional state of our employees, their workload, if they have everything they need for remote working, and if they have clarity on the business processes. In addition, in one of the latest surveys we asked employees how eager they feel about going back to the office and how comfortable they are with this idea, and also what are their major concerns regarding this process. This gives us a better understanding about specific circumstances people are in today and helps us to make decisions that are more balanced.

It is important to understand that this transition should be as comfortable for people as possible as their well-being is essential if the transition is going to go smoothly. These past few months of remote working have made us more human and kinder towards each other. We have become much closer as we have learned to talk openly not only about our work but also about some personal issues we face now. A connection we now have will help us in the coming months, as we will be going back gradually to our new reality.

RISKS AND VALUES

When considering coming back to work in the office, companies today need to weigh up the potential risks against the benefits. To avoid the risks of people becoming sick, and possible liability risks connected with any illness, companies today need to implement a complex set of measures.

Companies should consider the worst-case scenario if, for example, there are 400 people in an office and one of them tests positive for COVID-19. They will need to think about what measures should be taken to ensure that other people are safe and what will be the price of these measures for the company. If there are more risks than values from coming back to the office and if there's an opportunity to continue remote working for the coming months, then this would probably be the best option.

We all want to return to normal life as soon as possible, but in the current situation when we don't have immunity to protect us from the virus and don't have a vaccine, we need to be very careful and take care about the most valuable resource we have – our employees.

People will still value working from an office, but what they will appreciate most is flexibility. People have learned how to share their time more effectively between how they work and their personal and moving to flexible working hours will be a key benefit for organisations to stay competitive within the market.



Product excellence for a safer world through innovation





STRUCTURED CABLING SOLUTIONS **FOR BUILDINGS & INDUSTRIAL**

Norden Structured Cabling System provides a cabling infrastructure that delivers predictable performance as well as has the flexibility to accommodate moves, adds and changes; maximizes system availability, provides redundancy; and future proofs the usability of the cabling system.

COPPER SOLUTIONS | FIBRE SOLUTION | DATA CENTER SOLUTION BUILDING & INDUSTRIAL CABLES | FIRE RESISTANT CABLE & ACCESSORIES

NORDEN BRAND & PRODUCTS

'Eyenor' Surveillance system

'NVS' Public address system

'SECNOR' Access control system

'SAFENOR' Emergency exit system











A broad portfolio of storage solutions for smart video

We see what's next. Smart security is advancing faster than ever. Be ready with our thoughtfully calibrated storage solutions designed for smart video. From raw video to AI, endpoint to cloud, our products deliver reliability and longevity, support multi-streams and offer scalable surveillance capacities and built-in analytics—all from Western Digital.

Learn more at www.westerndigital.com/no-blind-spots



Available at







