JUNE 2021

CYBERSECURITY NEWS

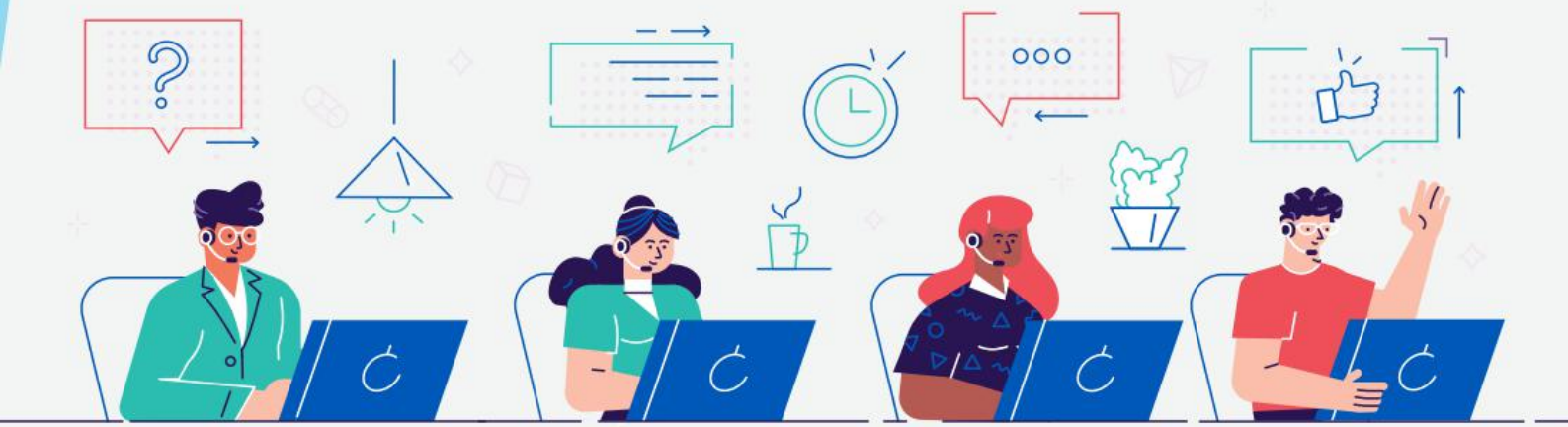
16 A LOOK INTO THE RECENT CYBERATTACKS

- LESSONS LEARNT -

TELEMARKETING SERVICES

We can help you!

- Achieve sales faster through outbound lead generation
- Regular followups with potential leads
- Appointment setting with your targeted customers
- Consistent data upgrade
- Inbound Call Center to turn inquiries into leads
- Marketing support to turn inbound inquiries into leads
- Gain insights from dormant customers and win them back
- Event Support
- Market research & surveys



+971 58 898 7360

www.qnamarcom.com

marcom_qna QNAMarketing QNA Marcom

CYBERSECURITY NEWS

PUBLISHED BY
QNA Marcom

HEAD OFFICE:
Office 1705, Grosvernor Business Tower, Barsha Heights (Tecom), Dubai, UAE.

CTO
Niket Raje
niket@qnamarcom.com
Tel: 971-4-5851684

GM - OPERATIONS
Suman Yadav
suman@qnamarcom.com
Tel: 971-4-5851684

EDITORIAL
Divsha Bhat
divsha@qnamarcom.com
Tel: 971-4-5851684

SALES EXECUTIVE
Gavin Dias
gavin@qnamarcom.com
Mob: 971-505399394

Nigora Sariboyeva
nigora@qnamarcom.com
Mob: 971-581268767

MARKETING
Ana Azfar
ana@qnamarcom.com
Tel: 971-4-5851684

DESIGN
Ali Raza
ali@qnamarcom.com
Tel: 971-4-585168

PRODUCTION
Bhawana Kishan
bhawana@qnamarcom.com
Tel: 971-4-585168

AN OPTIMISTIC APPROACH

Albert Einstein once said – 'In the midst of every crisis, lies great opportunity.' This is particularly relevant to the global pandemic, which has created opportunities and fuelled new ideas for the cybersecurity vendors and solution providers. The industry has been supportive of transforming pandemic-driven attacks into pandemic-fuelled innovation.

Although, cyberattacks have been the 5th top-rated risk according to Global Risk Report 2020 and have become the new norm across public and private sectors, the new techniques, and tools, could tip the scales in favour of defence. Cybersecurity News discussed with the industry experts what they believe to be the emerging security patterns for the next year – and how to help strengthen security in the coming years.

We hope you enjoy reading our inaugural issue! Stay Safe All!

Divsha Bhat
Assistant Editor, QNA Marketing Management LLC.

Management

Managing Director
Ankit Shukla
ankit@qnamarcom.com

COO
Pankajam Dev
pk@qnamarcom.com

CONTENTS

OmniClouds Redefining Cloud and Data Security

The COVID-19 pandemic has largely proven to be an accelerator of cloud adoption and has become a lifeline for many organizations looking to stay in business from home. However, it also raises concerns about a cyber-pandemic involving data breaches and disrupted operations. According to OmniClouds, most organizations hosting data or operating in the public cloud experience a security incident, with multi-cloud organizations reporting up to twice as many incidents vs. single platform adopters.

The COVID-19 pandemic has largely proven to be an accelerator of cloud adoption and has become a lifeline for many organizations looking to stay in business from home. However, it also raises concerns about a cyber-pandemic involving data breaches and disrupted operations. According to OmniClouds, most organizations hosting data or operating in the public cloud experience a security incident, with multi-cloud organizations reporting up to twice as many incidents vs. single platform adopters.

Vidhu Raveendran
Vice President – Networks & Engineering, OmniClouds

Addressing the Cloud Security Challenges

While the cloud helps many organizations improve their access to critical software apps and services, it has also introduced new challenges in maintaining strong cybersecurity. Some of the challenges listed by OmniClouds are Data Breach, Data Loss, Insider Threats, DDoS attacks, API Security, Disaster Recovery, a performance that impacts availability. "Due to the cloud's nature of sharing resources, cloud security gives particular concern to identity management, privacy & access control. Consequences of a data breach may include misconfiguration and inadequate change control, lack of cloud security architecture and strategy, insufficient identity, credential access, and key management, account hijacking, insider threat, insecure interfaces and APIs, and weak control plane," commented Vidhu Raveendran, Vice President – Networks & Engi-

neering, OmniClouds.

So how do we overcome some of the cloud security challenges listed above? Vidhu believes that as more organizations are transferring infrastructure and services to the cloud and adopting a multi-cloud strategy, cloud applications and data need a secure environment. But for all the benefits of a multi-cloud strategy, some challenges come along. "It can be difficult to secure a multi-cloud strategy because of the lack of visibility across hosts and services. Perhaps most intriguing of all, the data owner does not have physical access to the places and devices where that information is stored. This makes it easier for hackers to find exploitable vulnerabilities within an organization's infrastructure. OmniClouds solutions via the cloud, on-premises, or as a blended combination of both, Omni Remote connects Enterprise branches, teleworkers, and end-users securely and reliably to applications in the cloud or data centres around the world. A single-pipeline integrated architecture combines comprehensive cloud security, advanced networking, industry-leading SD-WAN, robust analytics, and simplified automation into one software solution," explained Vidhu. "A single layer of defence is not enough for today's constantly evolving threat landscape. OmniClouds secure solutions protect file servers detects malware pre-execution, during execution, and post-execution. File security solutions can be managed from the single management console, a cloud-based, unified threat management tool. Network Attack Protection improves the detection of known vulnerabilities on the network level," he added.

Optimizing Security for Financial Organizations

The major concern of financial organizations about the use of cloud computing, and public cloud, is data protection. Vidhu explains that OmniClouds understands that financial services companies have a lot to consider when moving to the cloud. "OmniClouds helps organizations to realize the benefits of these programs – all while protecting data and maintaining compliance. Moreover, working with its partners, OmniClouds offers an unmatched combination of industry and technical expertise that will provide recommendations about the cloud service platform that can be considered a great fit for financial services companies," he said.

Vidhu further elaborates that OmniClouds helps organizations move their IT operations to the cloud through migration, implementation, and managed services, investing time to understand each client's holistic, unique requirements. "OmniClouds knowledge of financial services regulations worldwide – and its experience in helping clients protect their systems and information – has enabled the company to create a library of best practices and practical approaches to security. OmniClouds continues to reassess those needs throughout delivery, ensuring that the company provides services that its clients can count on to help keep data safe, systems protected, and their organizations regulatory compliant," he commented.

Securing Your Network to Work from Anywhere

OmniClouds provides a secure solution for Work from Home (WFH) users & remote admin users. They can securely access all applications anywhere, from any device with unified security management. From transitioning to the cloud to managing an increasingly distributed workforce, it is more important than ever to secure users, apps, and data—without compromising the employee experience. "With OmniClouds Secure Access solution, you get a full cloud-delivered security stack with a global reach. This allows you to protect all users, anywhere, for each application, without the complexity and expense of data center-based security," said Vidhu.

He further explained that secure access to the web and SaaS applications is simplified and intelligent, cloud-delivered security. OmniClouds Secure Internet Access enables your users to access applications using direct internet access (DIA) without compromising performance. Protect every user, including remote and mobile users, against all threats—with the simplicity and scale of a single solution.

Breaking the Misconceptions

One of the biggest impediments to the transition to a cloud computing environment for many organizations is security. "Many people do their research in advance to learn as much as they can about the capabilities enabled by placing workloads strategically in the cloud. Unfortunately, there is a lot of conflicting or questionable information swirling around, and sometimes customers are harbouring inaccurate assumptions about what exactly "the cloud" is, what it can and cannot do, and what it takes to become cloud-ready," said Vidhu.

The common misconceptions, according to OmniClouds, are –

- Cost savings are the most significant advantage of the cloud.
- One size fits all.
- The cloud is a standalone solution.
- The cloud is not secure.
- The cloud's too complex – lose control, and you are stuck.

"It is critical to understand the fact that the adoption of the cloud is highly safe. OmniClouds maintains extensive security measures to strengthen organizations networks," he added.

Defence Ready

Countless examples of cyberattacks from the past have demonstrated extensive damage. "OmniClouds can help the organization choose the right path to cloud security and make sure the defence is ready," concludes Vidhu.

Taking Cybersecurity to New Heights

"We have the tools to provide effective prevention, but we also need the champions to guide organizations in using those tools to reduce risks and the potential for attacks," says Mitch Parker, Executive Director of Information Services, Indiana University Health.

Roles and Responsibilities

My roles and responsibilities at IU Health involve oversight of the information security program and associated activities. I supervise the risk assessment, third-party risk, information security project management, PCI compliance, change management, and threat intelligence and research. Our team also works heavily in policies, processes, procedures, requirements and contracting. These allow us to work across the organization with our customers.

Biggest Challenges in the Role

Before the advent of electronic medical records (EMRs), technology supported the business functions of a health system. This included functions such as Enterprise Resource Planning (ERP), finance, payroll, and business process automation. When EMRs came into use, a new set of challenges surfaced, including a proliferation of devices and patient portal security. The era of COVID-19 has brought two new challenges: the implementation of the 21st Century CURES Act Final Rule and the distribution of the patient care environment outside the walls of the clinic or hospital.

The 21st Century CURES Act Final Rule changes how we think about

Mitch Parker
Executive Director of Information Services, Indiana University Health

security. It requires us to provide patients data using application programming interfaces (APIs). This is a challenge for organizations used to less interactive methods of delivery, such as patient portals. Also, many of them have had very controlled ecosystems that did not include third-party programs using APIs to download patient data. This requires providers to expand their security toolkit to perform risk management.

A corollary to this challenge is the distribution of care outside of hospitals. The explosion of telemedicine was one facet. Another is the significant uptick in the use of internet of medical things (IoMT) devices for patient care. These devices remotely report on conditions such as glucose levels or CPAP usage using either Wi-Fi or cell phone service. Hospitals and health systems need to be able to ascertain, assess, and address risk on these devices. Telemedicine and the IoMT improve patient care. However, they need excellent monitoring and good security to mitigate the inherent risks in their usage. Not everyone has clinical engineering support at home.

Why do you think the plethora of breaches continue?

More often than not, the root causes of these breaches lead back to a lack of operational management and monitoring processes. While healthcare has spent billions of dollars on cybersecurity, we haven't fixed the systems themselves.

This is how numerous ransomware attacks that befell healthcare institutions worked: Organizations, for the sake of convenience, left ports and protocols open to the Internet, often for support purposes. They didn't have effective log analysis in many cases. In other cases, they didn't have resources available to close discovered security holes. Two-factor authentication to a remote desktop session or VPN using breached credentials is not as common as it needs to be. This has enabled attackers to go on the offensive, sometimes spending months scoping out targets and exfiltrating data before detonating ransomware in networks.

Investing money in two areas, secure architectures and operational management plans, would significantly reduce risks. Having secure architectures means that the system as a whole is analyzed to determine the appropriate security measures and countermeasures to protect the confidentiality, integrity and availability of data. Operational management plans provide the guidelines for proper system operation. Ideally, they will also provide methods to detect anomalous operation and address the root causes. They also provide means by which organizations can plan when and how to upgrade system components to address risks and build on a secure foundation.

How do you determine what technologies to invest in?

The decision comes down to how organizations assess risks. The risk assessments identify the gaps that need to be addressed at a macro level. Understanding the gaps and technology infrastructure to solve any issues will allow an organization to stay ahead of cybercrime. From there, organizations can leverage their peers, trusted sources such as Gartner or Forrester, or prior customer experiences, to identify technology solutions to meet their needs. Organizations normally find the solution that works the best, addresses their needs, and mitigates risks.

It takes a full understanding of the risks that organizations face, along with understanding the technology landscape, to be able to determine which solutions will work best for the environment they will be placed in. A solution that isn't a match will open up additional risks and leave the organization less secure.

Do you think there is enough focus on prevention?

No. We have put many systems in place without forethought on how to secure them or even manage them in a way to spot anomalies early. Most of the time, easily fixed security issues are the downfall of organizations. The attackers aren't using 0-day attacks most of the time because they do not have a need to do so. They are leveraging attacks that already work. They are also using stolen credentials.

While cybersecurity solutions perform well for what they do, they cannot stop everything. They also cannot replicate or understand all the application or business logic complexities of an ERP or EMR system. It takes significant business knowledge to be able to identify anomalies to discover insider threats. It takes log analysis to identify potential anomalies such as data exfiltration or unusual login activity that often preclude attacks.

We have tools at hand that can help. Cloud-based technologies allow us to develop and reproduce secure architectures in a fraction of the time needed even five years ago. Automation and Intelligent systems provide log analysis and correlation that once were the provenance of organizations with large security teams. Good operational plans can put controls in place to identify insider threats before they cause significant harm. Two-factor authentication is now a commodity easily deployed.

We have the tools to provide effective prevention, but we also need the champions to guide organizations in using those tools to reduce risks and the potential for attacks.

INTEGRATING THE THREE PILLARS OF CYBERSECURITY

People, Technology, and Process - Ts. Saiful Bakhtiar Osman, Head of IT - APAC, ASCENT Fund Services believes that combining these three aspects, if executed appropriately, will enhance the organization's readiness and overall IT security posture.

Covid-19 has triggered a huge turbulence. How did the IT department of ASCENT Fund Services respond? What tools and strategies were adopted?

Indeed, the Covid-19 pandemic had taken all companies globally by surprise, and most of them are still recovering from it. The traditional ways of business were put to the test, and the need of technology had skyrocketed as a lifeline for the companies to survive.

Fortunately, for ASCENT Fund Services, with the foresight and solid commitment from the Management, we had been able to withstand the impact of this unprecedented event.

Our Business Continuity Plan (BCP) had proven its worth, and the transition of staff from working on-site to working from home had been carried out very smoothly. The safety and wellbeing of all staff has always been the priority of the Management, especially during this pandemic times. CITRIX has been used as the primary workstation for all our staff to be able to continue their daily work from home, or from anywhere with internet connectivity.

The technology adopted also allows our services to remain reliable, available, and accessible to all clients and premium partners. It is during this critical time that we need to be closer to all our clients and help them to succeed in their businesses. Adopting the Managed Azure Cloud had enabled all our offices in Asia Pacific, namely, Singapore, Malaysia, Hong Kong, China, Japan, and Australia to continue serving our clients and partners without any disruption.

What factors are driving your IT decision making process this year? Has it differed from the decisions you were making last year? If yes, how?

As everybody could recall, last year was full of uncertainties due to pandemic and hence, the focus for us was more on getting a fast and effective business recovery. It was a reactive approach, but it needs to be flexible enough to deal with any situations, especially with the changes in the global business landscape. It was that moment; our carefully crafted Business Continuity Plan (BCP) and infrastructure were being tested in a 'live mode'. Everything fell nicely in place, and we managed to make sure all our services were available, reliable, and accessible to all our clients.

As for this year, our focus would be to strengthen the overall IT security posture and readiness for the company. This is essential as we would like to create a highly secured and trusted environment for our clients and potential clients to engage us as their financial services provider. I would also consider this year as a stabilization period because we need to make sure that we are able to sustain the performance and improve at any areas that needs attention.

Ts. Saiful Bakhtiar Osman
Head of IT - APAC,
ASCENT Fund Services

As for the medium to long term planning, is to explore the potential integration with Analytics and to bring in some Process Automation as a catalyst to push the business forward. This is because, we already have a pool of very experienced and dynamic team of analysts. By having the right Analytics tool, it would allow them to provide a better analysis, forecasting and advisory services to all our clients.

In addition, for Process Automation, if implemented correctly, would take away the manual and repetitive works which subsequently increases the efficiency of the existing process. By having automation in place, we could also increase manpower productivity, and we are able to reallocate our resources to work on other added value projects or initiatives.

Name one technology that was invaluable for you in the past year. How did it help?

If I need to pick one technology, then it would be Citrix. Citrix has been a great fit to our overall setup and to seamlessly connect all our offices across the Asia Pacific. As opposed to the traditional Virtual Private Network (VPN) setup, Citrix enables more functionalities to Admin to control all the devices in the organization.

Being an Independent Global Fund Administrator, we need to ensure that we are always in compliance with all the regulations and standards. Hence, data movement, access control and data security are among some critical aspects that we could achieve within the Citrix environment.

Nevertheless, the same technology may not be applicable to other organizations. My advice, it goes back to the Risk Appetite of your organization when adopting a technology. You should carefully weigh the Pros and Cons, practicality, as well as the intended ROIs. For instance, never decide to go for Cloud infrastructure just simply because it is the trend now and many companies are doing so. There is no 'one size fits all' type of solution. Choose the best technology that fits your own environment, because only you know the issues, the challenges, and the limitation of your own organization.

What is your advice on balancing security and digitalization?

My advice, have a proper plan in place, no shortcuts. Digitalization is not about converting your current process and make it digital. You would need to review back the current process, end-to-end, to identify any redundant processes, to make amendments, and to remove any unnecessary steps that have been in practice for so long. This refined process and your technology approach will determine the success of your Digitalization journey with the intended ROIs.

As for Security, it is not a compromise, even the budget for IT is being cut by most organizations, due to pandemic. Practice implementing a "Security-by-Design" approach in every projects or initiatives, so that we can do the things right, the first time. Else, you would expose yourself to unnecessary firefighting, once the projects go 'Live' in the Production, should there be any vulnerabilities to the system. If you failed to plan, then you are really planning to fail, because it would waste a lot of resources.

I have this BRAG rule of thumb, that I have been using when it comes to selecting the right balance and the right project:

B – Brings value to our Clients and Stakeholders. Noted that you may have a lot of projects in the pipeline, choose the best that would impact your bottom line or increase your Customers Experience (CX), etc.
R – Right fit for the organization. We do not want to overspend in this difficult time. You know your organization the best, so craft out something that best applied to your own environment.

A – Aligned with the Business Strategy and Business Goals. It is time for IT Heads to come forward as a reliable advisor to leverage the technology to achieve the business goals.

G – Good balance of People, Process, and Technology. A good system should be able to increase the productivity of the entire organization, and to get the intended responds from all your customers.

There is a lot of focus around cybersecurity and much of it around how to address and mitigate damage? Do you think there is enough focus on prevention?

There is no right or wrong when it comes to cybersecurity. As much as we should focus on prevention, the reality is that the rapid growing of the cyber threats, makes it almost impossible to keep up. Once you are equipped with the tools to prevent a known threat, a new one would emerge the next day. That is the reason why most companies are taking the effort to focus on how to address or mitigate the damage, should such incidents happen.

Personally, I believe that IT Security awareness is very crucial. You could not ignore the human factor, as it would turn out to be the weakest link in your overall security infrastructure. You may spend thousands building up the fortress around your company, but the threat would still be able to penetrate because of your own internal people. i.e.: A Staff may happen to click an email attachment sent by a bogus sender, which triggered the company's laptop to be encrypted by Ransomware.

Start building your strength around People, Technology, and Process:
People – make sure all your Staff are properly trained and continuously be reminded on cyber threats. IT Awareness should be an on-going program by the company and measurement of the staff's level of compliance and understanding.

Technology – to have sufficient protection with the right tools and technology, to mitigate and reduce the likelihood of cyber-attacks. You can always outsource to a reliable outsourcing partner should your staff do not have the right skillset for the job.

Process - all work process must be very clear for every staff to follow and these processes should be regularly reviewed to ensure it is up-to-date and relevant. The same also applies to policies and procedures, i.e.: how frequent that a staff needs to change the password, who can access what, clean desk policy, documents classifications, etc.

I am certain that with the combination of these three elements, if implemented correctly, would improve the readiness and the overall IT security posture for the organization. Subsequently, would protect and prepare the organization from the ever-increasing cyber threats.

STAYING AHEAD OF THE ATTACKERS

— By Divsha Bhat

Transforming the endpoint security with their pioneering Moving Target Defense, Morphisec protects businesses worldwide from the most dangerous and sophisticated attacks efficiently. Read on to more about the organization from the CEO, Ronen Yehoshua.

Over the last decade, cyber-attacks have become sophisticated with government and private organizations increasing spending to protect their data. Companies are extra vigilant of the potential threat from cybercriminals and investing in the security of the organization by embracing new technologies and specialized teams. To empower organizations of all sizes to stop their next breach, Morphisec launched a suite of solutions for endpoints, servers and cloud, that use patented zero trust runtime security powered by an innovative and patented technique called – 'Moving Target Defense'. This technique continuously changes the target parameters of a system to prevent cyber-attacks. This approach does not require employees to be security experts to tackle unknown threats. Besides, Morphisec enhances the existing security tools of the organization to make them more efficient.

By restraining attacks, Morphisec helps prevent the damage and the cost. The company is currently protecting over 7 million endpoints and servers.

"To stay ahead of the potential cyber threats, we shift the advantage from the attacker back to the defender. Instead of chasing the attackers, Moving Target Defense will make the attackers chase us. This technique continuously alters their attack surface and deceives attackers into exposing themselves," said Ronen Yehoshua, CEO, Morphisec. "We were fortunate enough to bring this technology to the table for our customers. We ensure that we immune the system with Moving Target Defense," said. With a simple to install and operate security system, Morphisec provides a unique value proposition of powerful protection combined with low total cost of ownership.

Morphisec's flagship solution – Morphisec Guard is a complete endpoint prevention platform that prevents the threats that are designed to bypass status quo prevention and detection tools. This solution completely maximizes Window's native security features and adds a zero trust runtime protection layer that has no performance impact. It runs autonomously so that the endpoints are guarded even when not connected to the organization's network.

Ronen believes that the challeng-

es for businesses have increased during the pandemic with employees working remotely using unsecured devices and connecting to cloud-based applications. "Morphisec Guard extends prevention capabilities through Moving Target Defense by creating a zero-trust execution environment. By creating a zero trust runtime environment, only trusted code can run, so advanced threats are prevented even when there is no known signature or behavioral pattern," said Ronen. "Aligning with the security needs of the organizations, we built this solution to secure the physical and virtual endpoints," added Ronen.

Servers and cloud workloads are prime targets for hackers. The company's latest solution, Morphisec Keep, prevents the most damaging cyberattacks on physical and virtual servers with critical exploit prevention and memory protection technology. "Morphisec Keep prevents zero-day and advanced attacks, without requiring any prior knowledge of the threat behavior. It keeps the servers protected from vulnerability exploits when patches are not yet available or deployed. Morphisec Keep also protects Windows and Linux servers regardless of whether they are on-premises or cloud," explained Ronen. Easy to roll out with no system conflicts and zero maintenance, Morphisec Keep does not generate false alerts and blocks attack pre-breach before they can cause any damage.

"To stay ahead of the potential cyber threats, we shift the advantage from the attacker back to the defender. Instead of chasing the attackers, Moving Target Defense will make the attackers chase us. This technique continuously alters their attack surface and deceives attackers into exposing themselves"

"We are proud to say that we bring in the best cybersecurity solution which is simple yet effective and with low total cost of ownership. With this new solution, we assure to stop advanced cyberattacks in organizations" he commented.

Talking about Morphisec's recent participation at Cybertech Global UAE with their partner Rheinmetall Group, Ronen said – "The United Arab Emirates is stepping up as a leader in digital transformation. But with this transformation, the country can be exposed to cyberthreats. At the event, we witnessed that organizations are aware of the increasing threats and are looking for preventive measures. Along with our partner Rheinmetall, we assure to help the customers from preventing them from being breached."

Morphisec states that over 77% of all cybercrimes target small and mid-sized businesses. Hence, it offers cybersecurity solutions for such businesses to protect them from sophisticated attacks. "Ideal from small to large enterprises, our groundbreaking Moving Target Defense prevents threats and reduces the organization's risk exposure without affecting business productivity. Moreover, Morphisec cloud delivered Security Center provides end-to-end visibility into organization-wide threats.

As the market evolved in recent years, Ronen explains that Morphisec realized the challenges faced by the CISOs and decided to introduce solutions that can make them stress-free. "We decided to put CISOs to a good night's sleep with our innovative solutions that can mitigate the threats which are out of their control." But he also believes that CISOs should take the first step towards security. "Considering all aspects of security, a CISO should secure the appropriate budget and resources. Every dollar counts! Hence a CISO should divide the budget equally in security. If the first dollar is spent on preventive measures, then a CISO will spend less on detection, hunting, and breaches and dramatically reduce the risk."

Ronen closes the note giving this piece of wonderful advice to the CISOs and looks forward to building a strong footprint in the region.

BEING PROACTIVE

Working on R&I provides organizational knowledge and expertise to better approach the technology gap, to make better decisions and to be more effective and accurate believes Jose L. Diego, Expert-Evaluator, Security Projects for the European Commission and Head of Project Management, Valencia Local Police, Spain.

• Describe your roles and responsibilities at Valencia Local Police.

I´m the Head of Project Management Division and my mission is to manage the research and innovation work on security in order to improve our police service to the citizenship in the medium and long term.

• What innovative technologies have been adopted by your organization?

Not only technologies, but also methodologies and best practices have been applied. Working on R&I provides organizational knowledge and expertise to better approach the technology gap, to make better decisions and to be more effective and accurate.

Technologies for improving forensics (intelligent sensors), for improving data management and operational organization capacity (platforms and systems), for engaging with victims and communities (software, APPs and e-trainings), for better responding to emergencies (platforms and also equipment), for better interventions (drones, etc)... It is a really long list and it is a non-stop work.

Jose L Diego
Expert-Evaluator, Security Projects for the European Commission and Head of Project Management, Valencia Local Police, Spain

• As the police, security framework at your organization must be unique. In such case, how do you manage the BYOD approach?

The security of our system and internal networks is a must for us, so BYOD is something strictly limited at this moment, both for legal and security reasons. Nevertheless, it is under permanent feasibility assessment by our Tech Unit.

• With organizations spending millions on cybersecurity, why do you think the plethora of breaches continue?

It is simple: they are innovating faster than us. Organizations and public bodies should take the lead in research and innovation to prevent these threats.

• What is your advice on balancing security and digitalization?

Step by step, any step forward must be ensured. Our security chain is as strong as the weakest link and no mistake is allowed. Of course, this entails to put more effort on R&I.

• There is a lot of focus around cybersecurity and much of it around how to address and mitigate damage. Do you think there is enough focus on prevention?

Prevention is the key; it is more effective, cheaper and prevents more damages than reactive strategies. R&I is a substantial part of prevention and a strong facilitator for implementing preventive policies.

• Tell us about your recent participation at Cybertech Global UAE. What did you present on?

At Cybertech Global UAE, I presented two of the European Projects in which Valencia Local Police is currently working in the area of cybersecurity: CC-DRIVER and RAYUELA. The sister projects are funded by the European Commission under the topic "Human factors and social, societal and organizational aspects to solve issues in fighting against crime and terrorism".

CC-DRIVER is a three-year EU-funded H2020 project which will combine interdisciplinary research with innovation activities to illuminate the role of technical and human factors in current cybercrime trends and translate the findings into co-design tools and innovative methods to support the fight against cybercrime. By developing a shared view of the whole cybercrime eco-system with its various actors and dimensions of cybercriminality, we can deepen our understanding of what we can do, collectively and individually, to address and overcome it. An ethical, data protection and social impact assessment will build trust in the public for the use of technology in cybercrime-fighting efforts and ensure the respect of privacy and fundamental rights of citizens.

RAYUELA is a three-year EU funded H2020 project whose main goal is to better understand the drivers and human factors affecting certain relevant ways of cyber criminality, as well as empower and educate young people (children and teenagers primarily) in the benefits, risks and threats intrinsically linked to the use of the Internet by playing, thus preventing and mitigating cybercriminal behavior.

About Jose L Diego

He is an expert-evaluator for the European Commission within 4 different initiatives:

- Horizon2020 – Secure Societies challenge
- DG JUSTICE Research Programmes
- DG HOME Research Programmes
- Radicalisation Awareness Network

He began his career as a consultant at Deloitte, and nowadays is the Head of Project Management in the Valencia Local Police, as well as International Lecturer, OSCE Hate crimes trainer & Liaison officer and also Professor for a Master on Human Resources, for two Masters in Criminology and for the Chiefs' Police Academy as well. He has managed 30 EU projects (including 14 H2020-Secure Societies projects) in matters like R&D, domestic violence, police mediation and training, community policing, forensics, youth offending, crime fighting, road traffic, police management, diversity, emergencies, environmental police, cybercrime, Police ICTs, hybrid threats, smart cities & security, etc. He holds Degrees in Law and in Criminology and a Master in Human Resources Management as well.

A LOOK INTO THE RECENT CYBERATTACKS

- LESSONS LEARNT -

— By Divsha Bhat

The year 2020 will go down in history as a year that no one might have imagined and that few will forget. The pandemic and the resulting national lockdowns have altered the workplace as we know it. According to a study, cybercriminals have benefited from coronavirus pandemic by tailoring their cybercrime campaigns to attract victims to pandemic themes and exploit people who work from home. Cyberattacks have been rated the 5th top rated risk in 2020 according to Global Risk Report 2020 and has become the new norm across public and private sectors. And according to their 2021 report, cyber risks will continue to rank among global risks.

- **81 global firms from 81 countries reported data breaches in the first half of 2020**
- **80% of firms have seen an increase in cyberattacks in 2020**
- **Coronavirus was blamed for a 238% rise in cyberattacks on banks**
- **Phishing attacks have seen a dramatic increase of 600% since the end of February**
- **Ransomware attacks rose 148% in March and the average ransomware payment rose by 33% to $111,605 as compared to Q4 2019**

Source: CyberReef

Notable Attacks of 2020

In January 2020, a hacker group named Shiny Hunters stole 25 million students' email addresses and passwords from a math solving app, Mathway. A report shows that the attackers put the data up for sale for $4,000 on the dark web on May 18, 2020. The passwords were encrypted, and the responsibility of decrypting them was on the buyers. Even if the data buyer cannot crack the passwords, having 25 million email addresses is still helpful for sending malware-laden phishing or spam emails to the students.

In May 2020, EasyJet admitted that they had been a victim of a highly sophisticated cyberattack in which 9 million customer's email addresses and travel details were stolen. The BBC report stated that the attackers were also able to access 2,208 customer's credit/debit card numbers along with CVV. Although EasyJet was aware of the data breach since January, it was able to notify customer's whose credit card details were stolen only in early April as it took time to understand the scope of the attack and identify who had been impacted.

According to researchers, two zero-day flaws were also detected in Zoom's macOS client version. The web conferencing platform vulnerabilities could give local, unprivileged attackers root privileges and allow them to access victims' microphones and cameras. The two vulnerabilities were later patched, according to Zoom.

Thousands of cyberattacks took place in 2020 and just as the year was about to end, along came the SolarWinds incident which immediately qualified for the most significant attack of the year. In a long campaign that began in March, a hacker group believed to be linked to the Russian government obtained access to computer systems belonging to multiple U.S. government agencies, including the U.S. Treasury and Commerce. The attack involved hackers compromising the infrastructure of SolarWinds. The hackers got access to emails at the U.S. Treasury, Justice and Commerce departments, and other agencies. The breach could have compromised up to 18,000 SolarWinds customers that used the company's Orion network monitoring software.

Even the most reputable organizations cannot promise adequate data security. Cybersecurity is a never-ending operation, which is why every major business maintains a cybersecurity team dedicated to data protection and preventing different forms of cyberattacks. However, there are many challenges and how do you think enterprises can strengthen their cybersecurity posture?

Tackling the Challenges

Lack of Cybersecurity Expertise: One of the most significant issues that companies face is a scarcity of trained staff to handle their security needs. According to Deloitte, the skill shortage is a part of a global problem where the cybersecurity workforce gap is expected to stand at 1.8 million by 2022. A proactive strategy for each company to develop and retain its cybersecurity workforce should be one of the organization's top priorities. Organizations should consider developing security talent naturally, as security expertise is becoming increasingly difficult to source and maintain. Organizations must also understand that the new technology workforce needs versatility.

Artificial Intelligence and Machine Learning: For the past few years, we have been unable to ignore the advantages of Artificial Intelligence and Machine Learning technology in various fields. Hackers may use AI to find vulnerabilities in high-value targets in a large dataset. After a lot of testing, AI can learn anomalies in behaviour patterns that can be used as a protective method – but sadly, hackers can use the same techniques to carry out a cyberattack. Handling AI-based threats and defending our AI properties from cyberattacks can be difficult now and in the future.

Every new cyberattack should not serve as a reminder to tighten cybersecurity throughout the organization. At all times, a response plan, timely upgrades should be prioritized. Cybersecurity training programs are required for an attentive approach. This can help people in general, as well as employees, detect potential threats.

Cloud: Because of the flexibility and costs associated with legacy data centres, businesses have started migrating their critical data to the cloud. Moving data to the cloud requires the correct configuration and security measures. The cloud security solutions include firewalls, multi-factor authentication, Virtual Private Networks (VPN), and others. In short, an enterprise must implement protocols and technologies to protect itself from both external and internal threats.

Security cannot be achieved solely by the CISO. It will need the complete support of the security team as well as the entire organization. To help develop their skills and, ultimately, to achieve business outcomes, the next generation of CISOs will need to take every opportunity to educate their colleagues about security best practices and how it is an enabler for achieving business outcomes.

What CISOs can do to help Cybersecurity Challenge?
• Obtain true visibility throughout your environment
• Develop a strong backup and recovery
• Get Proactive - Have a response plan in place
• Create risk-based security programs to encourage business agility
• Outsource cybersecurity to a company that specializes in it

Lessons Learnt

Every new cyberattack should not serve as a reminder to tighten cybersecurity throughout the organization. At all times, a response plan, timely upgrades should be prioritized. Cybersecurity training programs are required for an attentive approach. This can help people in general, as well as employees, detect potential threats. Recognizing and preventing phishing scams, ransomware attacks, and other threats as soon as possible can significantly reduce the damage.

Maintain Tight Cybersecurity Posture: Organizations should maintain a strong cybersecurity posture, which includes following industry best practices for password management and monitoring. Users must also update their passwords regularly and use complicated passwords. All organizations must also take a multi-layered approach to cybersecurity, think beyond the box, and remain updated with all security best practices, tools, and technologies.

Train your Weakest Link: Humans, it is said, are still the weakest link in cybersecurity. Hackers have exploited human vulnerabilities and weaknesses in the past. Employee phishing training and exercises must be conducted regularly to help combat and mitigate these incidents. Fake phishing attacks and annual employee training are essential for ensuring that the entire organization has a security-first mindset.

Response Plan: In the event of a cyber incident, all organizations should have a Cybersecurity Incident Response Plan in place to restore operations rapidly and efficiently.

Secure the Future

No system is safe but learning from these incidents can help better monitor, detect, prevent, and protect the existing IT environments. Limit internet access points with silos, test often and train your humans. Stay Secure!

A STREAMLINED APPROACH

M H Alshaya Co keeps things easy by using a single solution for all internal corporate communications across multiple markets. All other IT procedures fall into place as communications become more streamlined and efficient believes Patrick Pitchappa, Director – Information Security & Risk for the organization. Read on to know more...

Covid-19 has triggered a huge turbulence. How did the IT department of M H Alshaya Group respond? What tools and strategies were adopted?

Yes, there is no doubt that COVID-19 triggered huge turbulence across the globe, and we all had to learn to work in new ways. But as we approach the midpoint of 2021, I think we now have a 'new normal' BAU for IT departments.

The world is working from home (WFH) or remotely and we are successfully enabling this in many ways. Most of the measures we started in Q1 2020 have continued – some might be reversed but employees have learnt to work in new ways, and we are supporting flexible working going forward.

If I had to sum it up in one phrase then it would be 'The world has gone to the cloud'. All our communications including voice, video and text now go through cloud-based apps – that applies within the IT team and Alshaya Group as a whole. This has eased early WFH difficulties and has helped a WFH culture mature admirably in the past 15 months.

We wanted to keep things as simple as possible and identified one tool that we use across multiple markets for all internal business communications. With communications more streamlined and efficient, all other IT processes fell into place. Other time-tested strategies such as using a Virtual Private Network (VPN) and Virtual Desktop Interface (VDI) further drove the IT efficiency of WFH.

In the times that we are living now, what is your view of the role of cybersecurity function? What should it consist of?

Everybody with a Smartphone is on the Internet 24x7 and their usage moves fluidly across devices and platforms for work and in their personal lives. In this context, Cybersecurity is of fundamental importance. It's important to keep our work information, our personal information and our loved ones' information safe on the Internet. It's as basic as that.

Patrick Pitchappa
Director - Information Security & Risk, M H Alshaya & Co WLL

From a corporate perspective we follow the NIST Cybersecurity Framework of Identity, Protect, Detect, Respond and Recover to ensure we have a robust Cybersecurity programme.

With organisations spending millions on cybersecurity, why do you think the plethora of breaches continue?

Simply put, the threat actors out there are fifty steps ahead of most organisations in the corporate world. They pour in a lot of effort into targeting and breaking into the most recent or modern cybersecurity programmes.

Whilst they are doing this, the CISO has to justify their

IT budget and cybersecurity roadmaps to their Company's senior decisions-makers. Budgets for Cybersecurity tools, processes and personnel are allocated, vendor management processes or Request for Proposals (RFP) are followed before narrowing down on a vendor or tool. All this takes time and has the potential to impact any Cybersecurity roadmap.

With technology evolving at blazing speeds, organisations without proper cybersecurity leaders and practitioners will struggle to implement the proper cybersecurity practices for the latest technologies in a timely way. The threat actors take advantage of this to conduct cyber-attacks.

It's also true that many organisations are negligent or ignorant about cybersecurity, lacking proper cybersecurity policies, procedures, processes and personnel. And of course, when it comes to cybersecurity, people are the weakest link - 95% of cyber-attacks are caused by people, most times unintentionally by employees. In order to mitigate this risk, employee cybersecurity awareness must be carried out regularly for all staff. Taking all of the above into account, it's not surprising there are a plethora of cyber-attacks on a daily basis.

What is your advice on balancing security and digitalisation?

Any digital project or product must be built on a strong security foundation. That's how balancing of security and digitalization begins.

Zoom is a great example to cite. Initially launched with a weak security framework, Zoom had to go through a very hard time before they got their product secure. Meanwhile, they lost of a major chunk of corporate market share, which went to a relatively new product called Microsoft Teams in 2020.

Teams survived and thrived in the corporate world because it was fundamentally built on the best Microsoft 365 and Office 365 hyper-scale, enterprise-grade cloud, delivering advanced security and compliance capabilities.

How to get the foundation right? A proper security architectural review must be conducted on all digital projects and products as the first step. Then digital projects must go through a DevSecOps cycle to be secure at any given time. Doing so allows any vulnerabilities found to be quickly fixed before any threat actor exploits them. This will provide an overall balance to security and digitalization.

There is a lot of focus around cybersecurity and much of it around how to address and mitigate damage? Do you think there is enough focus on prevention?

As the old saying goes, prevention is better than cure. This is definitely true in cybersecurity also. When cybersecurity is in firefighting mode, then it's surely a failure. In order to proactively build a cybersecurity programme and improve the security posture of an organisation, these basic cybersecurity processes, programmes and tools must be implemented.

Get started with Next Generation Firewalls, IPS/IDS, End Point Detection and Response (EDR), followed by a robust Identity Access Management programme, a proper IT Asset Inventory platform, SIEM/SOAR, Privilege Access Management (PAM), Data Leakage Prevention (DLP), Web Application Firewall (WAF), DDoS Protection, Cloud Access Security Broker (CASB), Zero Trust Architecture, etc.

Additionally, conduct regular external and internal audits to evaluate yourself, conduct regular Red Team Exercises, use an external vendor partner for Vulnerability Assessment and Penetration Testing, build a highly competent CSIRT team, build a Cyber Defence Centre for Threat Intelligence and Threat Hunting, sign up with an external cyber risk score partner and also purchase cyber risk insurance.

This is not an exhaustive list but includes what could be described as the bare essentials for an effective cybersecurity programme that is focused on prevention.

The world is working from home (WFH) or remotely and we are successfully enabling this in many ways. Most of the measures we started in Q1 2020 have continued – some might be reversed but employees have learnt to work in new ways, and we are supporting flexible working going forward.

AN ADVISORY APPROACH

The advising methodology of CyberKnight helps customers understand where they are on the Zero Trust Security path today and where they need to be tomorrow. This high-level gap analysis helps to identify cybersecurity challenges, that can then be mapped to business outcomes, through technology adoption.
Read on to know more from Avinash Advani, Founder and CEO, CyberKnight

Covid-19 has changed the cybersecurity landscape forever. But how do you think this industry will transform post pandemic?

With the rapid shift to remote working, most organizations had to suddenly deal with decentralized cybersecurity, as the corporate perimeter extended overnight. Initially, this put many organizations on the back foot, as they had to reactively deal with cybersecurity issues without having all the necessary controls implemented. Over the course of the pandemic, organizations have been playing catch up to put the required measures in place to protect users and data, no matter where they are located, while providing the access to corporate assets, without introducing new attack vectors. This can all be achieved by Zero Trust Security, which will surely be the reference framework post pandemic, because although some users will need to go back to the office, many organizations have realized that providing a remote work environment reduces overhead and costs. In fact, more mature organizations have even started rolling out the next evolution of Zero Trust Security, the Secure Access Service Edge (SASE).

Avinash Advani
Founder and CEO,
CyberKnight

Also, over the course of the pandemic, cyber attackers took ad-

vantage of the increased attack surface by targeting remote users with social engineering and malware. This increased the overall number of cyberattacks globally. So, if security was a board level priority before COVID-19, it is now at the top of the agenda!

There is an increased focus on security models including Zero Trust. How are you helping your customers take protective countermeasures?

Zero Trust Security is deeply ingrained in CyberKnight's DNA. In fact, we built our portfolio from the ground-up on a Zero Trust Security foundation, and mapped market-leading vendor technologies to each of the ZTX Framework's micro-perimeters. When we speak to enterprise and government organizations, we do not start with a product discussion, but instead with a Zero Trust Security brief, which includes:

- Flaws in current security strategies and architectures
- Zero Trust Security assumptions
- Steps to achieve Zero Trust Security
- The components of Zero Trust Security and the benefits of the ZTX Framework
- The mapping of our product portfolio to the ZTX Framework

Our advisory approach assists customers to understand where they are on the Zero Trust Security journey today, and where they need to be tomorrow. This high-level gap analysis helps to identify cybersecurity challenges, that can then be mapped to business outcomes, through technology adoption.

Furthermore, this year we will be highlighting an important theme at GISEC 2021 to help customers transition from a reactive approach to a more proactive stance: "The Evolution of Cybersecurity to Cyber Resilience". A cyber-resilient company is one that can rapidly predict, prevent, detect, contain, and recover, minimizing exposure to an attack and its impact on business, against countless threats to data, applications, and IT infrastructure. Cyber resilience is all about anticipating. We believe that being ready for anything and Zero Trust is at the heart of cyber resilience. The technologies we will be showcasing at GISEC will enable regional customers organizations to simplify their incident response while achieving compliance.

Artificial Intelligence and Machine Learning have been driving innovation in cybersecurity. How can enterprises leverage these technologies to further automate network security?

Technology innovation in AI and ML has thus far been geared towards complementing humans in the security operations center (SOC). With the multitude of tools and data processing required to combat modern cyberattacks, combined with the industry's skills shortage problem, automation and orchestration across all cybersecurity domains using AI and ML, have become essential for organizations to implement Zero Trust Security. The ZTX Framework depends on continuous monitoring, proving every user, device and traffic flow, as well as logging and inspecting all traffic, all of which can be facilitated through AI and ML based network security automation.

Given all the challenges in the year 2020, what advice would you give your customers and partners on how to best navigate the coming years?

Other than implementing Zero Trust Security, it is also critical to mitigate manpower being the weakest link in an organization. This can be achieved by providing effective and ongoing security awareness and training, followed by measurable, actionable, realistic and time-bound assessments. Security controls should also be put in place to both empower the user to report security issues, while protecting them from cyberattacks using automated detection, prevention and response.

Also, if you analyze and dissect why there was an exponential increase in successful cyberattacks in 2020, besides the remote working attack vector, it can be observed that many organizations still did not have foundational security tools in place, and/or continued to expose vulnerable assets to attackers without patching them. So fundamental cybersecurity hygiene is essential.

Do you think there are cyber innovation stories that are not getting enough attention?

Cybersecurity is a hot market and a hot topic, so innovation in the space is definitely getting the required attention, especially with increased regulation around data privacy and compliance. Furthermore, cyber attackers always seem to be moving at a faster pace than cybersecurity tools, so in order to keep up, all eyes are on the industry's startups and innovators. Plus, companies like CyberKnight and the channel partner community invest heavily to bring next-generation cybersecurity solutions to customers by educating the market, creating awareness and evangelizing the latest cyber innovation. That being said, security awareness exists within the industry, within the IT domain to an extent, and within associated service sectors like financial markets, media etc. But the average consumer still does not take cybersecurity seriously, because either their knowledge about cyberattacks and the potential financial or reputational damage that can be caused is limited, or because they have not yet been a victim.

KEY VALUE: Sharing is Caring

Rahav Shalom-Revivo is the founder of the Israeli Ministry of Finance's Fintech-Cyber Innovation Lab, the world's first initiative that leverages government assets and data to promote Fintech and Cyber businesses on an open innovation platform. She is also establishing and managing a national Financial-Cyber International Partnership with international governments, regulators, and financial institutions worldwide.

Rahav Shalom-Revivo
Head of Financial-Cyber Innovation and International Engagements, Ministry of Finance - Israel

Tell us about your scope of responsibilities at Ministry of Finance as Head of Financial-Cyber Innovation and international Engagements.

I have established and am managing the Financial-Cyber Innovation and International Engagements unit in the Israeli Ministry of Finance. As such, I'm in charge of developing and creating valuable international relationships with ministries, financial regulators and financial institutions. One aspect to such activity is the Financial-Cyber Simulation that will be held at Dubai in the Expo, and that will allow different countries to discuss the financial impact of a dramatic cyber attack on the global financial eco-system. Another aspect of my work is to find new ways to support and embrace innovation – Fintech and Cyber startups through unique assets that we have as a government, including data.

I have joined the Ministry of Finance 3 years ago, after more than 18 years in the hi-tech industry, where I started as a Computer Software Engineer and then climbed up the management ladder and became an R&D senior manager.

In an age of advanced threats, what steps/ actions are you taking to mitigate the risk at your organization?

One key value that we have is information sharing. "Sharing is caring" and it can promote the organization's level of awareness to threats, vulnerabilities and even recommendations to mitigate an attack. When an attack occurs it usually do not target one financial institution or even one financial sector, and since our role is to support the protection of the entire Israeli Financial Eco-System, sharing information with these organizations, between them, and with international entities – is mandatory to really be secured.

Another perspective is to embrace and promote innovation, whether it is cyber innovation (in the "Israeli Cyber Nation") or whether it is Fintech innovation that on one hand promotes the capabilities of the market, but on the other we must make sure that it is safe and secured.

Can you explain in brief about the Fintech Cyber Innovation Lab?

Sure, this program grew from the understanding that we, as the Ministry of Finance, have at the Israeli National Financial CERT, not only very unique knowledge and understanding of the end-to-end financial processes, the threats and vulnerabilities that are associated with that, but we also have a huge data pool of Financial-Cyber data, most of it is non confidential and not personalized, and when bundling it all together – we can bring strong value to fintech and cyber startups.

Therefore, we joined forces with two other government entities – the Cyber Directorate and the Innovation Authority, each one brings its own unique expertise and ability to support the lab, and since we believe that we can never truly mimic the needs of the private sector, we published a tender in which Mastercard and EnelX won.

The FinSec lab is being built these days. The call for applications to startups is now open, and entrepreneurs that will join the lab will be able to enjoy not only the government's financial-cyber expertise and data, but also the governments

network of connections, monetary support, and knowledge and financial data that is coming from world leaders as Mastercard and EnelX. This is the first program in the world that leverages such government data and assets to the private sector.

Can you explain in brief about the Multilateral Financial-Cyber Simulation that will take place at Dubai's Expo?

"Collective Strength", The Multilateral Simulation is the climax of Financial-Cyber international engagements that bring the international collaboration and cooperation around Financial-Cyber and between Finance Ministers to the next level.

In this simulation Ministers of Finance or their deputies will sit together around one table and will discuss the financial impact of a cyber attack that harms critical international financial processes and it will enable the participating countries to engage together with their answer to such attack. We all know that a cyber attack can be as a pandemic – it crosses sectors and borders very easily, one country's problem becomes all countries problem very easily. We need to work together to overcome such an attack and in order to protect the stability of the domestic and international financial eco-systems.

The Israeli Ministry of Finance is leading the simulation, that will be held in Dubai's Expo, at the Israeli Pavilion, in December 2021.

The Finance Ministries of Germany, Italy, Austria, and the Netherlands will be participating, and we're in the process of engaging additional countries. The BIS is working with us on the simulation as well, and additional international organizations are expected to join.

What is your advice on balancing security and digitalization?

It is always a challenge – the need to move forward, to support the citizens and economy's needs, to utilize fantastic technological capabilities and at the same time we want to make sure that the financial eco system is stable, that it remains secured, and that we give more to our citizens but at the same time continue to protect them.

The last year of COVID 19 brought to us all accelerated digitalization processes, whether it was the need of employees to work from home in any device that they have and connect to the organization's secured systems, and our ability as consumers to connect to many services remotely, and to manage our money that way. The entire world is moving forward and as Satya Nadella, Microsoft's CEO said in April 2020 – "We saw 2 years of digital transformation in 2 months" and the pace is not slowing down.

We must continue and move forward, the future is here, but at the same time we must keep the financial eco system secured, stable, since the amount of online services grow, since the attack surfaces and the entry points for attackers grow, since AI is being developed – both in order to bring new capabilities and at the same time can be used for attacks, and since 5G is being implemented and everything will be connected to the internet.

What is your take on private-public partnership? Is it necessary?

It is not only necessary, but also mandatory. The fastest and most accurate way forward is by joining hands together, sharing needs and constraints and finding the win-win situation to us all. The Fintech-Cyber Innovation lab and the Regulatory Sandbox are an example to it, and many other programs as well.

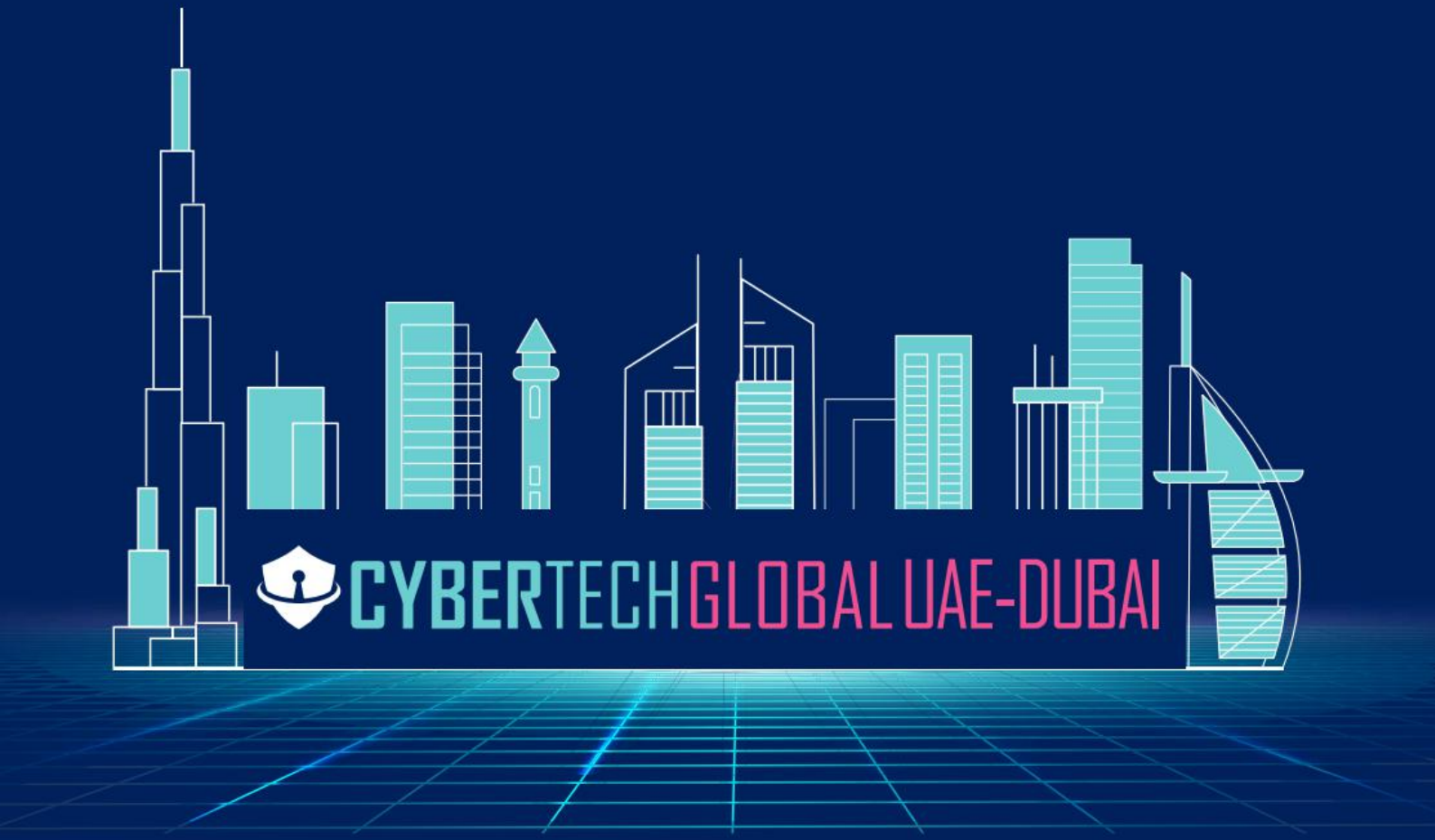
Any cybersecurity success stories you would like to share?

I would like to change the question a bit and refer to collaboration success stories. Cause only by joining forces together we can really make a valuable impact.

During COVID 19 outbreak, we have established the Financial CERTs forum. The forum consists of the Italian, Nordic, Switzerland and of course the Israeli Financial CERTs. We meet on a regular basis, sharing threats and vulnerabilities, new attack vectors and the outcome of these attacks, knowledge and understanding on the financial cybercrime players.

We have also accelerated the bilateral collaboration on Financial-Cyber and on fintech and cyber innovation and meet with Finance and Treasury Ministries from all over the world to share our intellectual property, methodologies, and threat intelligence. And last but certainly not least is Collective Strength - the Financial-Cyber Multilateral Simulation that will be held at Dubai and that will bring the collaboration to the next level. Only by joining forces together – we can win this Financial-Cyber war.

The Israeli Ministry of Finance is leading the simulation, that will be held in Dubai's Expo, at the Israeli Pavilion, in December 2021.



Cyber in a World of Change

Organized by Cybertech Global Events, the 8th edition of renowned international exhibition and conference and the largest networking event for the cyber industry outside the US – The Cybertech Global UAE was held from April 5th -7th 2021 at the Grand Hyatt, Dubai. Featuring thousands of cybersecurity experts from around the world, the event included lectures, plenary sessions, VIP speakers, in addition to an extensive exhibition for companies of all sizes along with a startup pavilion dedicated to young and innovative start-ups.

The forum included 120+ global speakers who addressed the cybersecurity challenges and strategies and repercussions in a wide range of sectors and disciplines such as fintech, retail, insurance, aviation, economics, and politics. The event was a first of a kind with decision makers sitting around the same table, including participation from the DP World, the Israel National Cyber Directorate, FAA, EuroControl, Emirati Airlines, Israel Shipyards, and others.

Leading experts in the global cybersecurity community participated in Cybertech Global-Dubai, either physically or virtually. Among them were Mohamed Hamad Hareb Al-Kuwaiti, Head of Cybersecurity - UAE Government, Yigal Unna, Director General, Israel National Cyber Directorate, Gen. (ret.), David H. Petraeus, Former Director of the CIA, Ann Johnson, Corporate Vice President, Cybersecurity Solutions Group, Microsoft, among others.

The official marketing agency for the event was QNA Marketing Management LLC.

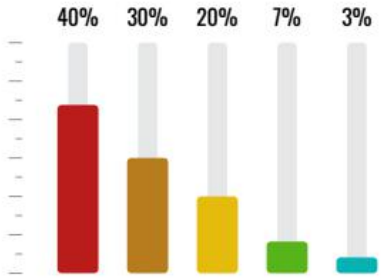
The conference sessions included key topics like Artificial Intelligence, Advanced Internet of Things, Blockchain, Cloud, Big Data, and focused n a wide spectrum of different sectors like healthcare, banking and finance, etc.

SECTOR SPECIFIC TOPICS
• Maritime & Logistics in the cyber space
• The post covid challenges in the healthcare sector
• Aviation in the cyber space
• Smart Buildings, Smart Cities, Smart Nation
• Secrets of Unit 8200 – Incubator Forging Entrepreneurs and Innovators
• Building an innovative and cyber ecosystem

The Cybertech Global UAE will return for a second year in a row from March 28th – 30th 2022. Together with their partners, the event looks forward to breaking the boundaries of global innovation.

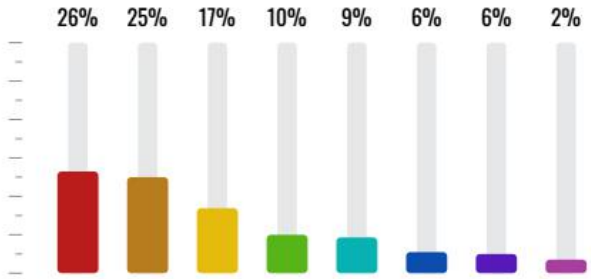
Cybertech Global UAE 2021 Statistics

COUNTRY



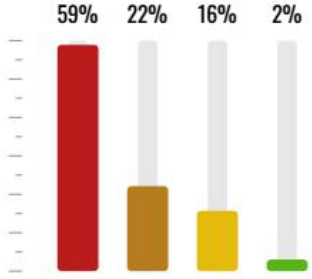
UAE	40
UK, Slovakia, India, Italy & over 60 others	30
Israel	20
USA	7
Germany	3

VERTICALS



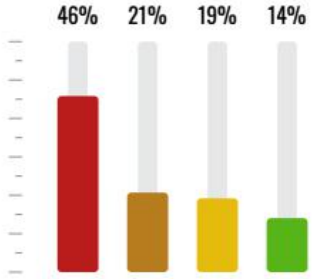
Finance	26
Gaming, HR, Retail & Others	25
SCADA	17
Aviation	10
Smart City	9
Health	6
Telecom Communications	5
Maritime	2

PURPOSE OF VISIT



Meet Potential Partners/ Networking	59
Knowledge Acquisition	22
Investment	16
Technology Acquisition	2

POSITION RANK



C-Level, VP, Executive	46
Others	21
Mid-Manager	19
Engineer, Developer, Programmer & Technical Team	14

Source: CyberTechGlobal UAE-Dubai

MOVING SECURITY OPERATIONS CENTERS UP IN THE MATURITY LADDER

Security Operations Centers have been the most widely discussed topic by cyber security professionals across the globe in the last few years. Security Operations Center aka SOC is an integral element of an organization's cyber resilience capabilities. SOC plays critical role in proactively detecting and responding to variety of cyber threats to which an organization is exposed. In addition, SOC in organization also handles responsibilities such as assessment of various cyber threats, selection and implementation of various security incident and event monitoring (SIEM) solutions, end point security management, Incident Response etc.

How conventional SOC is built & operated in an organization?

Setting up and operating a conventional SOC in an organization is a costly and time-consuming process which involves the following activities:

- Implementation of SIEM Solution
- Development of Use Cases
- Integration of Devices with SIEM Solution
- Creation & Implementation of SOC Playbooks
- Staffing the SOC

Implementation of SIEM Solution

Implementation of an SIEM (Security Incidents & Event Management) solution is the foundation of setting up SOC in an organization. A SIEM solution helps an organization in managing security incidents faced by them by reviewing the huge pile of logs generated by endpoints and applications owned by an organization. The conventional log management task requires a lot of manual effort for reviewing the logs. With the help of correlation engine, SIEM solution simplifies the task of log reviews. SIEM solution collects critical systems related logs, machine data from their IT ecosystem and helps in analyzing, identifying and responding to suspicious activities which could result in potential security incidents. The following are the capabilities of standard SIEM solutions available in the market:

- Log Management
- Threat Monitoring & Detection
- Incident Response & Threat Mitigation
- Threat Intelligence Integration
- Threat Analytics & Reporting
- Vulnerability Assessment

Vimal Mani
CISA, CISM, Six Sigma Black Belt,
Head of Information Security
Department of Bank of Sharjah

- Endpoint Security Management
- Digital Forensics

Development of Use Cases

Once SIEM solution is implemented, the list of use cases/scenarios to be identified which will be eventually configured into SIEM solution to start tracking the logs related to those use cases/scenarios. Relevant use cases can be identified from MITRE ATT&CK Framework which is the repository of TTPs (Tools, Techniques, Processes) used by adversaries such as hackers. Business & IT environments need to be considered in selection of the right set of use cases from the large volume of use cases available for reference.

Integration of Devices with SIEM Solution

SOC Administrator/ Security Head should plan and decide on which devices will send data to the SIEM solution and what should be the scale in terms of events per second and storage required. It is very critical to ensure that the data sent to the SIEM solution is well structured and linked with specific use cases for which it is intended. Integration of various applications, appliances with SIEM solution need to be planned into 2 to 3 years roadmap which will help the SOC team in fine tuning the log monitoring process carried out by the SIEM solution. All the supporting infrastructure required need to be identified and implemented. Antivirus, Endpoints, IDS/IPS, Firewalls, EPP, EDR kind of security devices /appliances need to be integrated with SIEM solution to have a seamless incident response.

Creation & Implementation of SOC Playbooks

SOC Playbook is a critical tool used by SOC Administrators in analyzing and responding to a security incident. SOC Playbooks will be generally drafted in the form of checklist with details steps that need to be taken to successfully respond to specific security incidents such as Ransomware, DDoS attack etc. These steps will have manual as well automation tasks to be performed. Having such detailed steps, these SOC Playbooks help in planning the automation of SOC Operations. So, we can consider SOC Playbooks as end-to-end response for specific types of security incidents. So, organizations need to develop and maintain different SOC Playbooks in their SOC to manage different types of incidents. These SOC Playbooks need to be revisited inline to the TTPs used by adversaries such as hackers.

Staffing & Operationalizing the SOC

Based on the operating model of the SOC, staffing options need to be explored and appropriate actions need to be taken. SOCs can have 5 *8 and 24 * 7 models of operations which the organizations need to decide based on their risk appetite and risk tolerance limits. If SOC is completely outsourced nothing to worry about staffing options which will be the responsibility of the outsourcing partner. Workstations required for the SOC staff need to be fixed with all the support software utilities and hardware required for them to perform their day-to-day operations. Staff of SOC needs to be provided with awareness on Incident Management Policy & Procedure of the organization. Also they need to be trained in Malware Analysis, Malware Reverse Engineering, Digital Forensics kind of domains closely related with SOC Administration.

Modernizing and improving the maturity of SOC Operations

It's critical for organizations to validate the effectiveness of SOC in periodic intervals with respect to Incident Management objectives of the organization. There are well defined SOC Maturity Models existing in practice which can be considered for benchmarking the current performance levels of SOC in an organization. Assessing the maturity of SOC operations and identifying improvement opportunities are very critical for every security leader. Based on the maturity we can classify the SOC Operations into the following categories:

- **First-generation SOC:**
SOC will only monitor the device logs wand event logs sent to the SIEM solution. No playbooks and incident response will be available. At this maturity level, SOC operation will be more of reactive natured.

- **Second-generation SOC:**
Second-generation SOC will use the data correlation capability which will convert the log data into security events which can be easily tracked and responded by teams deployed. At this maturity level, SOC operation will be more of reactive natured.

- **Third-generation SOC:**
Third-generation SOC will have more capabilities such as vulnerability management and compliance management. At this maturity level, SOC operation will be more of proactive natured which will have well constructed playbooks, information on lessons learnt which will help in handling incidents that will emerge currently as well in the future.

- **Fourth-generation SOC:**
A fourth-generation SOC is the one which will be equipped with all the latest state of the art security and monitoring technologies. At this level of maturity SOC operations will leverage Threat Intelligence Management, Vulnerability Management, Analytics, Artificial Intelligence, Machine Learning, Cyber Forensics, SOAR kind of technology elements which will help in delivering much higher value added SOC services.

To move from one maturity level to another, efforts required need to be planned well and executed failing which will not help the organizations in advancing their

SOC Maturity further. As a first step in such transition, existing SOC capabilities need to be assessed against the standard list of capabilities of SOCs operating at various maturity levels. SIEM, Logging, Reporting, Endpoint Security, DLP, Analytics, Network Security, Intrusion Prevention, Threat Intelligence & Vulnerability Management, Incident Response are some of the critical capabilities of a SOC. Industry Best Practices, standards, guidelines and frameworks for SOC operations need to be referred in doing this gap analysis.

Orchestration & Automation is the road to maturing the SOC Operations

SOC requires right data to analyze the events and provide responses in timely manner. Unfortunately, the processes of collecting and interpreting the data elements is being very weak in many of the contemporary SOCs.The SOAR (Security Orchestration, Automation, & Response) Technology arrived in market recently helps SOCs in resolving this and providing effective responses to security events. SOAR solution extends the capabilities of SIEM solution with inclusion of capabilities such as case management, orchestration, automation, and response. The objective of a SIEM solution is collecting and analyzing log data which also interpret data-based patterns of suspicious events. The objective of SOAR solution is grouping the existing log data from the SIEM solution and converting events into meaningful cases. Organizations want to improve their SOC maturity should invest in both SIEM/SOAR solutions as the combination of these will deliver much higher value. As a response to the increasing market demand, most of the SIEM solution vendors have started acquiring or developing SOAR capabilities within their security product lines.

In addition to having SIEM, SOAR solutions organizations should plan to have endpoint detection and response (EDR) solution also as part of their SOC Maturity Improvement Roadmap. With an EDR solution integrated with SIEM & SOAR solution, SOC can start collecting logs from endpoint devices, monitor the endpoint devices for suspicious events, and respond using SOAR solution through the use of the EDR endpoint client. SOAR solutions have Workflow and Collaboration, Ticket and Case Management, Orchestration, Automation and Threat Intelligence management capabilities. The combination of these capabilities will help an organization in improving the productivity and incident response capabilities of its SOC and the overall SOC Operating Maturity (Level 3 and Level 4).

Automation of SOC Playbooks

In many of the contemporary SOCs, the Playbooks are still only manually implemented. Automation of SOC Playbooks will be big catalyst towards improving the productivity and operating maturity of SOCs. Automation of SOC Playbooks will reduce the time-consuming work of SOC staff which they can utilize in addressing more complex analysis. Automation of SOC Playbooks can also help in improving the incident response to events reported by SIEM solution as the entire incident response will be automated with the help of automating the SOC Playbooks.

Conclusion

The industry has evolved significantly in managing cyber threats over last few decades with the help of continuous benchmarking of the statuesquo against industry best practices as well the experiences of those who has improved the maturity and transformed their SOC Operations. A low maturity SOC will always have the risk of failing to secure the organization so that hackers can easily target the organizations by exploiting the vulnerable security operations. Having an effective and high maturity SOC will help the organizations in managing and addressing wide range of cyber threats emerging in wake of Covid 19 created pandemonium in business. Hence, it's advisable for organizations to consider augmenting the existing capabilities of their SOC by bringing in new technologies such as SOAR, EDR and automating the SOC Playbooks. The cyber space is being a constant battlefield for last few decades with newly emerging threats and threat actors. If we don't improve the maturity of our SOC Operations we tend to become obsolete in our defense against cyber-attacks and have to face the loss of business and reputation. We need to keep the axiom "**Security is a journey, not a destination**." in mind and start working towards improving the maturity of our SOC operations in continuous manner.

Simplified Security

With the mission to empower the world to reach its full potential securely, Cisco intends to be the most trusted partner of its customers by offering effective security solutions. Fady Younes, Cisco's Regional Cybersecurity Director for the Middle East and Africa, says he and his team will keep working relentlessly to ensure that their customers are successful and secure in an uncertain, hybrid environment.

• Covid-19 has changed the cybersecurity landscape forever. But how do you think this industry will transform post pandemic?

Cybersecurity has increasingly been a boardroom topic over the past years – and it now became business critical. When the pandemic first hit, companies and organisations ensured first connectivity – then they thought about Security. Now, as we are preparing for a hybrid world environment, leaders want to make it right – and decide for an integrated, automated Cybersecurity posture.

A little over a year ago, we announced our platform Cisco SecureX. At the time, we knew it was an important technology, but we had no idea just how valuable it would become for so many organizations. Today, more than 7,000 customers are using SecureX to maximize the efficacy and efficiency of their security operations. And our journey to reduce complexity continues as customers keep moving to the cloud and consolidate their Security vendors.

• There is an increased focus on security models including Zero Trust. How are you helping your customers take protective countermeasures?

Access now happens everywhere—how do you ensure secure, trusted access and mitigate breaches when they inevitably occur?

A comprehensive zero-trust architecture requires each person, device, unit of data, network, and workload to earn and maintain your trust before being granted access. With zero trust, it's exponentially harder for an attack to progress from where its breached.

Our approach for zero trust is to establish trust, enforce trust at the point of access and continuously verify that the connection can still be trusted. Cisco Zero Trust protects your workforce, workloads and workplace with a balance between security and usability:

• **Workforce:** Protect against phishing, compromised credentials or other identity-based attacks with Duo's multi-factor authentication (MFA) to verify user identities and establish device trust before granting access to applications. We've recently announced our passwordless authentication solution, as part of our wider secure access offerings with industry leading MFA.

• **Workloads:** Secure hybrid, multicloud workloads and contain lateral movement with application segmentation. Detect software vulnerabilities and block communication to reduce your overall attack surface. We've also recently announced real-time, unified, workload and network security–an industry first.

• **Workplace:** Identify threats and maintain control over all connections over your network, including Internet of Things (IoT) devices with Software-Defined Access (SD-Access). Build safe and seamless experiences across your distributed workplaces to adapt to anything.

Cisco has been named a leader in Forrester's Zero Trust Wave report, and we are continuing to provide simplified, secure solutions to help our customers stay protected.

• Artificial Intelligence and Machine Learning have been driving innovation in cybersecurity. How can enterprises leverage these technologies to further automate network security?

The Cybersecurity industry is evolving to handle the rapid increase in the volume of threats, expanding attack surfaces and the accessibility of hacking.

Already today, our customer's systems see more than 20 billion cybersecurity threats every day or 250'000 every second.

Reinventing networking technologies is the only way to defend the internet and our digital society.

To stop more attacks, you must see more attacks, and you must

Fady Younes
Regional Cybersecurity Director for the Middle East and Africa, Cisco

see further. Cisco, through its Threat Detection arm, Talos, sees and analyses 2.2 Trillion Artifacts and blocks 10.5 Billion malicious events daily. Ultimately, this volume of data and analysis enables intent-based, self-driving, self-healing networks. A network that can redirect traffic on its own and heal itself from external shocks, such as cyberattacks.

Cisco's unique position as the leading networking vendor allows us to analyze huge amounts of data, from telemetry to traffic patterns, and understand anomalies as well as optimal network configurations.

In a world where bad actors move quickly, time to respond or the ability to bring rapid protection to close off multiple attack vectors instantaneously is crucial. Cisco's AI/ML work and connected portfolio approach allows our solutions to rapidly move information and optimal configurations to the holistic IT environment.

• Given all the challenges in the year 2020, what advice would you give your customers and partners on how to best navigate the coming years?

2020 has been a challenging year for many of us. We've learnt a lot together and realized now more than ever before that our future needs to be inclusive. And, without security, the dream of an inclusive future is just that — a dream. Our customers and partners understand the need to extend the opportunity of connectivity to everyone, and with security at the foundation of all they do.

In the coming years, Cisco will continue to support customers and partners in the challenges they face and to help them drive an inclusive future for all. This year, we conducted a double-blind study with representation of 25 countries and over 4,800 respondents across many industries and sectors. We combined the results (and formed the secret to a successful security practice!) and shared these in our 2021 Security Outcomes Study. In summary, we found that a proactive, best-of-breed tech refresh strategy allows customers to keep up with business growth. Additionally, a well-integrated tech stack improves recruitment and retention of their security talent. If customers and partners want to achieve overall program success, they should devote resources to proactive tech refresh and integrate their technology. And, if they want a strong security culture that's embraced by all, then the recommendation is to focus on good equipment, clear direction, accurate alerts, and timely fixes of security issues. We encourage our customers and partners to take a look at the full report for more recommendations to help bring success to their organizations in 2021 and beyond.

• What are your plans for the year ahead?

Our mission remains unchanged - empower the world to reach its full potential, securely. We want to be our customers most trusted partner by providing effective security solutions. My team and I will continue to work relentlessly in making our customers successful and secure in an uncertain, hybrid world.

Cybersecurity:
Building It the Right Way!

To address risk comprehensively, organizations must have a strong cybersecurity risk management and governance approach across the board. Organizations also require a complex standard that addresses security management, policies, procedures, network architecture, software design, and other vital safeguards, says Suresh Nair, Regional CISO - META Region, GE

• Covid-19 has triggered a huge turbulence. How did the IT department of GE respond? What tools and strategies were adopted?

As the impact of Coronavirus (COVID-19) continued to grow, we monitored the situation and aligned our plans and actions across GE. Our Digital Technology team convened a multi-functional group to coordinate support readiness as we had more employees working from home during this time. We ensured the network capacity to support an increasing number of employees needing remote connectivity as our top priority. We also worked on optimizing the work from home experience and encouraged users to use collaboration tools for sharing and storing files. We also implemented business continuity processes and workflows to support users who need emergency laptop devices to work from home. Our Service Desk and field services teams were equipped to handle larger volumes of support requests. Our IT teams have stepped up in major ways to support the business as we've navigated the challenges resulting from COVID-19.

• In the times that we are living now, what is your view of the role of cybersecurity function? What should it consist of?

Cybersecurity is a critical function for every business - no business wants to be a victim of a cyber-attack. Businesses should have an effective Cybersecurity plan in place to prevent cyber-attacks. Building the right cybersecurity team structure is crucial to managing risk and cost. Each organization has its own unique needs, and the structure will vary based on a company's size,

Suresh Nair
Regional CISO - META Region, GE

revenue, and employee headcount. Still, there are critical areas that should be prioritized for maintaining a basic cybersecurity posture, Risk Management, Security Operations, Security Architecture as well as Security Culture & Awareness.

• With organizations spending millions on cybersecurity, why do you think the plethora of breaches continue?

Unfortunately, one of the biggest sources of a data breach isn't some unknown or security bug, it's human error. Organizations need to have a robust cybersecurity risk management and governance program across the enterprise to address risk in a comprehensive and consistent manner. Additionally, organizations need a multifaceted standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

• What is your advice on balancing security and digitalization?

In the race to digital transformation, more and more organizations are turning to new technologies and serverless architecture to accelerate productivity. In turn, strategically managing data privacy, security, and compliance is crucial.

Most organizations require multiple cloud providers or environments (private, public and hybrid) to support the variety of applications, services and geographic distribution of their business. Here there is a need for consistent approach to data security across these varied environments.

As more high-profile data breaches are coming to light, so is new regulation with huge ramifications and penalties. Transformation requires a proactive approach to digital security. It is very important that businesses create a scalable and adaptable digital journey encompassing a well-defined digital strategy. It is also imperative for organisations to also manage the risks that are introduced into the environment and its impact to the existing ecosystem to drive optimum value from their digital initiatives. Despite all the above challenges and risks, organisations cannot overlook the opportunities that digitalization brings forth along with the profound impact that it shall have on them.

• There is a lot of focus around cybersecurity and much of it around how to address and mitigate damage? Do you think there is enough focus on prevention?

Incident response is integral to threat mitigation. I believe mitigation-based tools, on their own, simply can't provide the level of security needed to keep an organization secure. Detecting the breach early and taking active steps immediately will go a long way in limiting the impact of an attack. On average, most threats go undetected for upward of 100+ days. Effective cyber security is not just about tools and technological solutions; it is paramount to develop careful strategies tailored to the company's operations and risks. I believe the most important aspect of cyber security is prevention. Security and Risk Analysts know that attacks should be considered as a matter of when, where and how, and not if. Organizations need to develop and adopt best practices that support an effective, enterprise-wide security strategy to prevent cyber-attacks. One of the most important requirements is that cyber security should be an integral part of corporate governance, supported by senior management and proper funding.

For any organization starting off focusing on prevention, they should investigate CIS controls. The CIS Controls (formerly known as Critical Security Controls) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. This can safeguard their systems and data from known attack vectors. It can also be an effective guide for organizations that do yet not have a defined security program. Finally, in many cases, cyber-attacks are traced back to human error. The best way to combat this threat is to create a risk-aware workplace culture, and that starts with cyber security awareness. Prevention, however, should not replace detection and response. As with most areas, balance is necessary. Organizations need to supplement existing defenses with deep learning technology to prevent attacks before they can cause harm. The reduction in handling an incident for an IT team is worth the investment.

"Unfortunately, one of the biggest sources of a data breach isn't some unknown or security bug, it's human error."

HEIMDAL AI DISCOVERS A COMPLEX PHISHING CRYPTOCURRENCY SCAM CAMPAIGN

The cryptocurrency scam operators have been preparing their malicious campaign months in advance. Victims defrauded of 0.3 ETH and face long-term risks as well.

Cryptocurrencies have been tremendously growing in popularity, which never fails to attract cybercriminals. While there are still legitimate transactions and investment opportunities in this fintech niche, there are also a lot of shady deals covered up by the anonymity of cryptocurrency, or even downright scams.

We have warned our readers about cyptocurrency scams before and advised them on how to safely invest in cryptocurrency from a security standpoint.

Today, our AI engines and the team of malware analysts and machine learning engineers who are actively working to continuously improve the PredictiveDNS capabilities powering our Heimdal Threat Prevention suite (for Endpoints and Networks) have uncovered a sophisticated new and vast phishing cryptocurrency scam campaign. We are revealing the entire scheme here of tracking these malicious hackers across multiple domains and websites.

How the Malicious Scammers Prepared the Ground for their Theft Campaign.

The way this entire phishing campaign was planned out gives testimony to a remarkably organized group. The cybercriminals prepared the environment for their fraudulent campaign many months in advance with fake news websites about cryptocurrency.
This way, they could increase their ranking across search engines and be trusted as legit and trustworthy websites, as well as amass a readership of people interested in cryptocurrencies.

The registration addresses for all of these, while fake (rented out), span across UK, USA, Iceland, The Netherlands and more. The complexity of the campaign was carefully constructed to fly under the radar.

- https://primeinfos.com/ -> 2020-11-04 20:14:33 UTC
- https://inworldtalk.com/ -> 2021-01-26 13:13:26 UTC
- https://bitcocity.com/ -> 2020-11-04 20:14:33 UTC

Pavin Varughese
Country Manager - GCC,
Heimdal Security

- https://realtimebit.com/ -> 2021-01-26 13:13:28 UTC
- https://newspay.net/ -> 2020-11-04 20:14:38 UTC

The Purpose of the Phishing Cryptocurrency Scam Campaign

After laying the ground and building the trust of both search engines and readers, the cyber-criminals created several infected websites and shared them on fake news websites with articles like the following:

- https://primeinfos.com/news/2021-crypto-give-away-with-bitupporfolio/
- https://bitcocity.com/bitupporfolio-bitcoin-has-become-a-good-long-term-investment/

• https://inworldtalk.com/tag/bitupporfolio-com/

Our AI algorithm was able to discover the following phishing domains from the fake cryptocurrency news websites:

• geowexbit.com -> 2021-03-08 19:11:37 UTC
• changebitc.com -> 2021-04-02 09:09:56 UTC
• bitctoo.com -> 2021-04-05 22:11:17 UTC
• geocryptonium.com -> 2021-05-03 23:00:59 UTC
• chillbtc.com -> 2021-04-09 12:49:24 UTC
• bitcmax.com -> 2021-04-16 17:28:16 UTC
• excoinbit.com -> 2021-04-01 15:01:10 UTC
• hugobitc.com -> 2021-04-30 11:43:43 UTC
• coinsray.com -> 2021-02-06 12:06:28 UTC
• bigbitc.com -> 2021-04-08 10:58:49 UT
• highbitc.com -> 2021-04-08 10:58:57 UTC
• frexcoin.com -> 2021-01-06 15:43:06 UTC
• bitelix.com -> 2021-03-05 17:06:13 UTC
• cryptonsky.com -> 2021-02-20 23:49:12 UTC
• bitcoinist.com -> 2011-04-25 13:53:36 UTC -> Updated Date: 2021-04-13T12:53:05Z
• bitacex.com -> 2021-03-09 10:31:44 UTC
• https://fast-bitcoin-doubler.com -> 2020-11-27 09:07:10 UTC
• https://wibexlive.com -> 2019-02-23 07:00:30 UTC
• https://waukeen.io -> 2018-09-21
• https://cryptoreet.com -> 2021-02-26 22:46:29 UTC
• https://traderydefi.com -> 2021-03-16 15:32:06 UTC

You can notice the complexity of the campaign judging by the variety and the age of these domains as well. We believe the hackers might have hijacked some formerly legitimate domains as well in order to include them in the campaign (considering how old the registry dates for some of these are – like 2011, for instance). These malicious domains promise their readers that they will gain 8 ETH (Ethereum coin) if they can validate that the victim first sends them 0.3 ETH.

After completing the transaction, the money is lost and the data of the victim is likely stored for use in future cybercrime campaigns. The online Ethereum wallets of the hackers seem are empty right now, but this is probably part of a strategy to move funds and cash them in as soon as they receive them.

At the moment, none of these domains are reported elsewhere as being infected, which means that the cybercrime campaign hasn't been discovered by other cybersecurity researchers so far.

With the internet as vast as it is, traditional cybersecurity research methods are of course only able to discover a small fraction of cybercrimes committed, and even fewer of these are discovered before they can do serious damage.

Without the help of our advanced PredictiveDNS AI engine within Heimdal Threat Prevention, it's very likely that a long time would have passed until this new phishing cryptocurrency scam campaign was revealed.

5 reasons why having an MSSP is better than in-house Security?

Mohammed AlHarsousi
Managing Director of
CyberGate Defense

Threats of cybersecurity are real and creating havoc where ever they find vulnerabilities. The last year broke all records of cyberattacks lurking around companies and succeeding most of the time. According to Purplesec, in COVID-19 cybercrime went up 600%. In such volatile times, companies are torn between wanting to have an appropriate cyber defence mechanism and not bleeding money because of it. This dilemma resurfaces every time companies have to decide whether to invest in an in-house security team or opt for Managed Security Service Provider services.

Managed Security Service Provider is a third-party arrangement that renders their expert services for various forms of cyber and network security creating an environment safe from cybercrime for your organization.

"As a member of the cybersecurity community for the past many years, it has been my first-hand experience that companies who opt for MSSP strive better in the market as opposed to the ones with in-house teams. Outsourcing these services enables organizations to focus better on growing the businesses and use their time productively for business opportunities while letting the experts handle the threats and appropriate defence to the experts."

— Mohammed AlHarsousi, Managing Director of CyberGate Defense

Here's a breakdown of why MSSP is important and why choosing to go for MSSP is a better option for your company.

Cost-Effectiveness:
One of the main reasons why outsourcing MSSP services is a better option is that it is cost-effective. Having the necessary tools, equipment and expertise in-house collectively creates a big dent in your company wallet whereas with MSSP you only have to pay a certain fee for cyber-secure infrastructure that is already in place for various clients.

Paying the fee is closer to getting the higher end of the rope when you take into account the finances as paying upfront for technology investments is not a low number. This also prevents you from the additional hiring and employee cost which in itself is a time-consuming and laborious task. With the time saved from conducting interviews, hiring, choosing salaries with benefits and perks, holistically you end up saving a huge chunk of money.

Variation of tools:
A Managed Security Service provider will be equipped with a top-notch incident response centre and excellent tools to detect attacks before any harm is done. It is impossible to match the variation of security tools, advanced solutions to thwart attacks, and other external threat intelligence that an MSS provider entails.

Specialized Services:
Having an efficient MSSP ensures round-the-clock cyber-secure defences for your organization. With their expert opinion and valuable insights, you get a better understanding of the dangers of the cyber world and how to stay protected from them.

While an in-house team would have probably covered 3-4 areas of cybersecurity, an MSSP provides holistic services that take care of all possible cyber threats including detecting vulnerabilities in the system, proactively predicting incoming threats, responding timely, and quarantining reported emails.

Moreover, the maintenance, misconfigurations, and application bugs will all be catered to by your selected MSSP.

Easy Scalability:
What makes having MSSP worthwhile is also the fact that when your needs expand and change, you do not have to incur cost on updating processes and technology to fit your requirement but simply put up a request with your service provider to scale your cybersecurity defence strategies up a notch. With MSSP, you can go back and forth as per your requirements without having to worry about an increase in cost or any money going to waste in case of temporary scalability.

SERVICE PORTFOLIO

- Targeted database building
- BANT leads (Budget, Authority, Need, Timeline)
- MQL (Marketing Qualified Leads)
- ABM (Account Based Marketing)
- Wishlist appointment fixing
- Digital leads
- Digital Marketing
- Roadshows
- Exhibitions
- Public Relations
- Media Buying

+971 58 898 7360

www.qnamarcom.com

marcom_qna QNAMarketing QNA Marcom

QNA

CISCO

SECURE X

Simplify your security with the broadest, most integrated platform.

SECURITY

OUTCOMES

Visit cs.co/SecureX to learn more