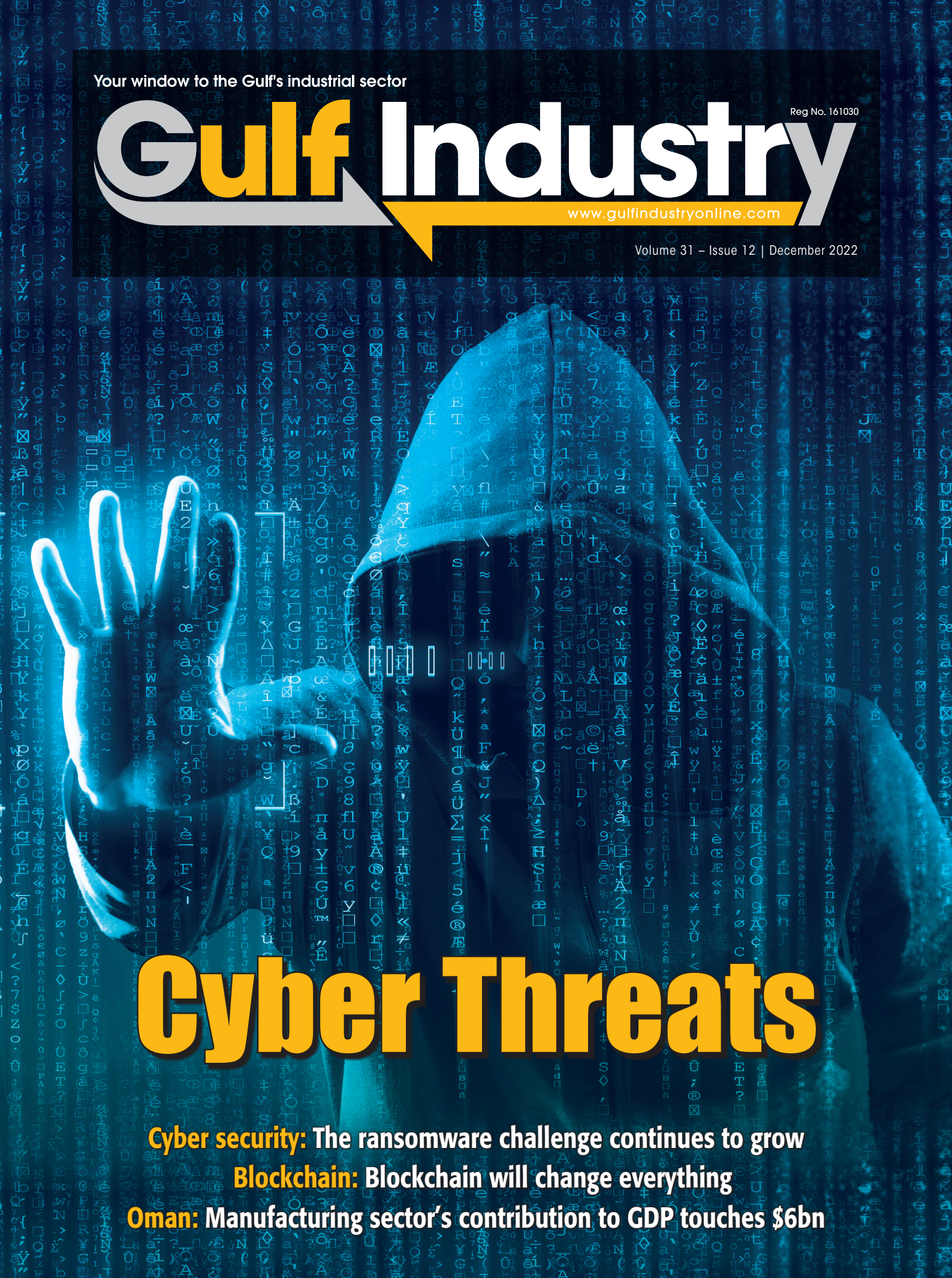
Your window to the Gulf's industrial sector

Gulf Industry

Reg No. 161030

www.gulfindustryonline.com

Volume 31 – Issue 12 | December 2022



Cyber Threats

Cyber security: The ransomware challenge continues to grow

Blockchain: Blockchain will change everything

Oman: Manufacturing sector's contribution to GDP touches $6bn

Global cybersecurity experts to convene in Bahrain

Industry-wide collaboration is high on the agenda of the Arab International Cybersecurity Summit (AICS) – a first-of-its-kind event being held in Bahrain from December 6 to 8 at Exhibition World Bahrain

Global cybersecurity experts are set to visit Bahrain this week to attend Arab world's pioneering cybersecurity event, the Arab International Cybersecurity Summit (AICS) – a first-of-its-kind event being held from December 6 to 8 at Exhibition World Bahrain.

Co-hosted by the National Cyber Security Centre and held under the patronage of His Royal Highness Prince Salman bin Hamad Al Khalifa, Crown Prince, Deputy Supreme Commander, and Prime Minister of the Kingdom of Bahrain, AICS represents the region's highest level of engagement, bringing together experts from government, industry, and business verticals including BFSI, oil and gas, energy, utilities, IT and telecommunications, manufacturing, education, and more.

The Summit's three-day Cyber Leaders Forum, which has attracted decision-makers from across Europe, the USA, the UK, Asia, the Baltics, and the Middle East, will look to reframe the region's Cyber Security Leadership landscape with Dr Mohamed Al Kuwaiti, Managing Director of the National Data Centre under the UAE's Supreme Council for National Security, expected to call for supercharged collaboration in his regional keynote address.

"With the cost of cybersecurity incidents in the Middle East reaching a new high of $6.93 million per data breach — significantly higher than the global average cost of $4.24 million per incident – it's time to question whether we move the action dial from defence to offence," Al Kuwaiti said.

> **"Nowadays, there are more devices than humans and hackers are getting more creative, making it difficult to implement efficient cybersecurity measures**

"With co-operation at the heart of the ACIS theme, we need to explore the best practice and importance of working together as a regional team to develop strategies to quickly evolve our security space to address the pressing concerns of today and for years to come," he added.

With the guidance and expertise of Dr Jassim Haji, President of the AI Society, delegates will also explore whether the increasing adoption of Artificial Intelligence is fuelling cybersecurity breaches.

"With almost all aspects of the industry now utilising the power of AI, there is a pressing need and demand for AI-driven tools to combat AI-driven attacks. This conference will help us better understand the aspects of AI and machine-learning, which could be hijacked for the cyber-attacks of the future," he explained.

The Forum will also look to explore how to change industry attitudes towards cybersecurity. Roshdi Osman, Cybersecurity Strategist of Saudi Aramco and founder of cyberleadership.org, will help delegates scrutinise the rationale for establishing a business enabler risk-based cybersecurity programme.

"Nowadays, there are more devices than humans and hackers are getting more creative, making it difficult to implement efficient cybersecurity measures," he said.

And as the Arab world increasingly regulates personal data use, the Forum will drill down into the role of regulations in safeguarding data, privacy, and security with the help of Karolina Mojzesowicz, Deputy Head of Unit Data Protection, European Commission.

"With all services moving to the cloud, it is the role of regulations to ensure that citizens' data is safe and secure, and regulators must always be mindful while drafting laws that they need to focus on ensuring data processing is lawful, fair, and transparent to the data subject," she said.

The dilemma of talent gaps in the cybersecurity sector will also come under the Forum's microscope with Dr Viktor Polic, Chief Information Security Officer, International Labour Organisation, looking to guide leaders along the pathway to talent development and upskilling.

"The current cybersecurity skill and ca-

pability gaps constitute a systemic vulnerability in the world's cyber resiliency. To solve this and create a robust digital economy system, it will be essential to create an inclusive cybersecurity workforce," he said.

The Forum will also feature virtual sessions from headline speakers Steve Wozniak, the co-founder of Apple, and Marc Randolph, co-founder and former CEO of Netflix. Complemented by a Block Stage platform to probe technical aspects of specific topics, Room 42 will host specific executive and technical sessions through table-top exercises, simulation games and live demos, including the use of a Velociraptor, an advanced digital forensic and incident response tool that can perform targeted gathering of digital forensic evidence, to triage hosts on a network.

The Hack Arena activation zone will be running a 'Capture the Flag' team competition on ethical hacking and cyber awareness. Consisting of 125 multi-disciplinary cybersecurity challenges, the competition is designed to test the users' capability across the entire spectrum of cybersecurity skills. The winners will receive prizes while all participants will be awarded a certificate of attendance and a personalised breakdown of their progress and achievements.

The summit will look to reframe the region's Cyber Security Leadership landscape

Trying to drive the importance of good internet habits, there will also be a cyber hackathon for university students, a cyber scavenger hunt for high school students.

The summit is set to host some of the industry's leading industry players, such as Forcepoint, Kaspersky, Axonious, Veritas and more. AICS is jointly organised by Messe Frankfurt Middle East and Bahraini event specialists Faalyat WLL and enjoys the support of Bahrain's Ministry of Interior, the Bahrain Economic Development Board, and the Central Bank of Bahrain. The event is sponsored by Benefit, Waterfall, NGN International and STC.

To find out more or register to attend, please visit: www.arab-cybersecurity.com ■

Cybersecurity is a serious business

CYBERSECURITY champions Hilal Computers are delivering infrastructure and a suite of software offerings to enhance the options available to businesses across the GCC .

The company boasts a dedicated managed Network Operation Centre (NOC) and Security Operation Centres (SOC) which they have established in association with partner company North Star Group in Bahrain and Saudi Arabia. The NOC and SOC recently received the highly prized SOC2 certification with the AICPA's (American Institute of Certified Public Accountants) TSC (Trust Services Criteria).

"We ensured that Hilal's managed NOC and SOC facility underwent the rigorous auditing process to ensure that we were maintaining the high standards that we have set in cybersecurity defence and protection. Our team of security analysts monitor thousands of security incidents each day. The award recognises the capability of our dedicated team of analysts," comments Shijas Mohidheen, Director Cyber Security for Hilal Computers.

In addition to the NOC and SOC, Hilal offers numerous security monitoring and protection software in collaboration with market leaders.

Hilal Computers are members CyberArk Partner Network to enhance their cyber footprint in the region. This offers organisations in the GCC, the CyberArk Identity Security Platform to secure human or machine identities across business applications, distributed workforces, hybrid cloud workloads and throughout the DevOps lifecycle.

Shijas Mohidheen

Another of Hilal's bouquet of cyber software is Vectra, the leader in threat detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito platform accelerates threat detection and investigation using Artificial Intelligence (AI) to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time.

Vectra AI recently awarded Hilal Computers and Hilal CTTC the accolade of Technical Partners of the Year in Bahrain and KSA, respectively.

"We are passionate about our status of defenders against cybersecurity violators. We understand that for many companies the Covid-19 pandemic exposed physical security and risk management gaps that senior business leaders are anxious about. We are happy to share our knowledge and expertise with a free consultation to any company looking to develop a strategy to plug the gaps in their defence from cyber-attacks and infiltration. Hilal together with North Star Group have developed a bouquet of services that provides international customers with cost effective SOC services and cyber security offerings of a global standard," adds Mohidheen.

He will catch you if you let him

Frank Abagnale, renowned cybercrime and fraud prevention expert, bestselling author and subject of the movie ***Catch Me If You Can***, spoke about identity theft and simple strategies to protect against cyber criminals at the recently held Black Hat MEA 2022 in Riyadh, Saudi Arabia.

Hackers only look for opportunities and open doors

Frank W. Abagnale Jr. has become a folk hero since the picturisation of his life in Catch Me if You Can. Frank Abagnale was played by Leonardo di Caprio and his captor in the FBI was played by Tom Hanks which has no doubt added to his star appeal.

A reformed poacher turned gamekeeper, Abagnale has been teaching at the FBI Academy for over 46 years and had the opportunity to teach two generations of FBI agents and conducted more than 3000 seminars around the world.

Speaking at Black Hat Middle East and Africa 2022 in Riyadh, last month, Abagnale gave the benefit of his wisdom to the prevention in cybersecurity fraud. *Gulf Industry* was privileged to witness his insights – here are some excerpts from his presentation:

MY PHILOSOPHY: PREVENTION, VERIFICATION & EDUCATION

Prevention, because once you lose your money, you will probably never get your money back. They may arrest the person, they may convict the person, they may send them to jail. But it is not likely you'll get your money back. If you make it easy for someone to steal from you, it's unfortunate, but someone will. In the US, we have seen more than $110 billion ordered for restitution that is still outstanding … today 91 per cent of that money will never be collected.

Verification because today anything can be replicated, duplicated, counterfeited. So before you part with any money or with any information you absolutely need to know who's on the other end of that device.

Education is the most powerful tool to fighting crime.

IDENTITY THEFT

We have seen a 73 per cent increase in the US in identity theft since the pandemic began. We have a victim in the US every two seconds.

In the world, in 2018, there were 3.6 billion identity records that were compromised, more than 14 billion identity records are available today on the dark web. That means probably everyone in this room, including myself, has already had their identity compromised.

Every breach occurs because someone did something that weren't supposed to do, or someone failed to do something they were supposed to do. Hackers do not cause breaches. Hackers only look for opportunities and open doors.

RANSOMWARE

In the 2,500 cases of ransomware in the US, more than $350 million was paid out by companies and cryptocurrency for being victims of ransomware. It is very simple as long as there is cryptocurrency, there will be ransomware. You cannot have ransomware if you didn't have cryptocurrency, so as long as there is cryptocurrency, we will continue to have ransomware.

Frank W Abagnale

PHISHING EMAILS

I have probably looked at over 15,000 phishing emails in my career. And up until a couple of years ago, they were always very easy to spot, not so much anymore.

Here is a real example from a technology company in Southern California with 4,000 employees. It is supposed to be an email from the CEO of the company, to the CFO of the company. And it simply read. Good morning, Jeff. Wonderful dinner at your home last night. Please thank your wife, Helen for me, my wife, Susan, and I truly enjoyed your company. As I mentioned to over dinner, I'm travelling this week to Nashville, Tennessee to attend a conference. So I will be out of the office till next Monday. I forgot to mention to you that I need you to wire these funds this morning for me to our client. Here's the information – Robert.

How was it created – Well, there's a picture of the CEO on Facebook picture of

>>

>>
his wife and children with their names. There's a picture of the CFO on Facebook, his wife and children, with their names. And of course, when he said he was going to the conference two months earlier, he said it on Facebook that he would be attending and how long they would be there. They're taking information from social media in real time and converting it into a phishing email. So exact and so precise and so simple to research.

Phishing emails are nothing more than social engineering. And the fact is, there is no technology, there never will be any technology including AI that can defeat social engineering. You can only defeat social engineering through education.

WEAK SPOTS

I could go in any company in the world, any company whether it be a fortune of 100 or 500 or Frank's plumbing shop with 12 employees and I'll find the same soft spots. There are soft spots, vulnerabilities, everywhere. Even in your own home, you have a refrigerator tells you how much milk is in it, you have a thermostat you control from 1000s of miles away, you have cameras around your house, and when you leave, you can go on your iPhone and look at your property. You have a device that you can talk to and ask what's the weather today or order this from Amazon, all of those devices can be hacked, manipulated, they are weak spots.

We develop a lot of technology around the world. But unfortunately, we very rarely vet that technology.

WHY USE PASSWORDS?

I hate passwords, every book I've ever written. I said I hate passwords. Passwords are for treehouses. They were invented in 1964, when I was 16 years old before I did any of the things I did. I am 74 years old, and we are still using passwords. How is that possible when we know that 63 per cent of network intrusions are compromised user passwords.

Half of the US was simply closed down by a compromised password. 81 per cent of hacking related breaches are weak or stolen passwords and 579 Password attacks happen every single second of every day, or 18 billion attacks a year.

If we take the three largest banks in the US, just the three largest names, they spend over $100 million a year just resetting passwords in their call centre at a $70 a reset. Why are we still using passwords? Well, I'm glad to say that passwords are going away.

This year, Microsoft, Google and Apple are going to install pass key every Apple phone in the world by the end of this year, that'll enable people to use the pass key technology and get away people from using the simple password or memorising the passwords.

EASY SCAMS

Millennials are scammed far more often than elderly folks; only elderly folks lose more money because they have more money to lose.

Unfortunately, what I did 50 years ago as a teenage boy, is 4000 times easier today. I didn't have all the technology we have today. So for me to forge a cheque, I needed a printing press colour, separations, negatives, plates, typesetting, and the skill to operate the press. Today, I open my laptop, I create a cheque in a few minutes, I go to the company's website, I capture their logo, I put it on the cheque, I make the cheque as fancy as I want as many colours as I want.

Unfortunately, we live in a too much information world which is accessible to all. So if I call that company and ask their bank transfer instructions, they tell me where they bank and give me that information, they even carry this information on their invoices. If I call their corporate communications, they send me a copy of their annual report. And on page three of the signature, the chairman of the board, the CEO and the CFO, the treasure trove of white glossy paper, black ink, I scan it, put it on the document that opens the doors to company. I wouldn't never believe that 50 years ago, but I can tell you what I did 50 years ago is now 4000 times easier to do today. ■

The Security Challenge

EVENT attendees at Black Hat MEA 2022 got the chance to hear testimonies about cybersecurity and its implications from an exciting line-up of world-renowned speakers from leading companies including CISOs of Boom Supersonic Chris Roberts.

Here, Roberts, gives key questions for businesses to consider for their cybersecurity needs. Excerpts from his speech at Black Hat Middle East and Africa 2022:

- **Do you have a firewall?**
- **Is it out of the shrink wrap and turned on?**
- **Is it configured for your needs?**
- **Stop believing that security can be 100% secure.**
- **Stop thinking that its hacker proof.**
- **If the very first time you have tested your incident response planning, is when you get breached. That's not cyber security.**

How many of you are inside organisations or working with companies that simply don't know where all of your assets are, don't know what's on them, don't know who has access to them and don't know what that purpose is? Buying new technology doesn't fix that. Taking a step back and looking at it differently will help. Take a look at how we can change our views on the security. Challenge what's out there.

Chris Roberts

When you talk to a vendor, start by asking them about the worst case scenario. Start asking them what happens if something occurs, what happens when the software goes in? What happens with the challenges? What happens if I get breached? Are you next to me as a true partner or are you going to stop blaming somebody else?

We have to challenge the very industry itself to change, because it's going to take every single one of us to do it. We have to get better at talking with each other, not at each other, but with each other.

Excerpts from Black Hat Middle East and Africa 2022.

Ransomware challenge hits manufacturing sector: survey

Even as the sector reported one of the lowest rates of ransom payment, the manufacturing sector reported paying the highest average ransom amount as against the cross-sector average ransom

Manufacturing is an attractive sector to target for cybercriminals

The ransomware challenge facing manufacturing and production organizations continues to grow. The manufacturing and production sector had the highest average ransom payment across all sectors, according to a new report from Sophos.

According to the newly released "The State of Ransomware in Manufacturing and Production" survey report, the manufacturing and production sector paid an average ransomware payment of $2.036 million in 2021, more than double of the cross-sector average estimated at $812,360 during the same time period.

Even as the sector reported one of the lowest rates of ransom payment, with 33 per cent paying out compared to the global average of 46 per cent. At the same time, the sector reported paying the highest average ransom amount at $2.036 million as against the cross-sector average ransom was $812,360.

The report found 66 per cent of manufacturing and production organisations surveyed reported an increase in the complexity of cyber attacks, and 61 per cent reported an increase in the volume of cyber attacks when compared to the previous years survey.

The increase in complexity and volume is also 7 per cent and 4 per cent higher than the cross-sector average, respectively.

Diving into the ransom payments further, manufacturing and production has one of the broadest spreads of ransoms across all sectors, with respondents reporting a wide range of payments: one in ten (11 per cent) paid less than $1K while nearly one third of the respondents (37 per cent) paid more than $100K. 8 per cent of respondents paid above $1M or more.

"Manufacturing is an attractive sector to target for cybercriminals due to the privileged position it occupies in the supply chain," said John Shier, Senior Security Advisor, Sophos.

"Outdated infrastructure and lack of visibility into the OT environment provides attackers with an easy way in and a launching pad for attacks inside a breached network. The convergence of IT and OT is increasing the attack surface and exacerbating an already complex threat environment," he added.

He pointed out that while having reliable backups is an important part of recovery, today's ransomware threat requires a detailed response plan that includes human-led threat hunting capabilities," he said.

John Shier, Senior Security Advisor, Sophos

"Complex attacks require comprehensive protection, which, for many organisations, will include the addition of managed detection and response (MDR) teams who are trained to look for and neutralise active attackers," said Shier.

The Sophos survey involved 5,600 IT professionals in mid-sized organizations across 31 countries, including 419 respondents from the manufacturing and production sector.

50PC FIRMS HIT IN 2021

In 2021, the survey found that 55 per cent organisations in the sector reporting being hit by ransomware, up from 36 per cent the previous year. Sophos said this shows that hackers have become considerably more capable of executing the most significant attacks at scale.

The rise in successful ransomware at-

>>

>>
tacks is part of an increasingly challenging threat environment that has affected organisations across all sectors. Respondents across all sectors reported an increase in cyberattack volume, complexity, and/or impact.

Manufacturing and production has been particularly impacted by the changing threat landscape, with 61 per cent of respondents reporting an increase in the volume of attacks on their organisations over the last year (vs. 57 per cent cross-sector average) and 66 per cent reporting an increase in attack complexity (vs. 59 per cent cross-sector average).

"It may be that the sector's superior ability to stop data encryption has forced adversaries to up their games when it comes to attacks. Alternatively, it may simply reflect an increased focus on the sector by cyber criminals over the last year," the report said.

LOWEST LEVEL OF BACKUP USE

Manufacturing and production companies reported the lowest level of backup use across all sectors, with just 58 per cent of respondents using this approach to restore encrypted data compared to the cross-sector average of 73 per cent.

In fact, the sector reduces the use of backup compared with the previous year, when 68 per cent of organisations used backups for data restoration. This is a concerning finding as backups are essential for recovery from ransomware and many other incidents.

Furthermore, almost half of respondents (48 per cent) reported using other means to restore their data.

> **Outdated infrastructure and lack of visibility into the OT environment provides attackers with an easy way in and a launching pad for attacks inside a breached network**

The percentage using backups, paying ransom, and using other means clearly adds up to more than 100 per cent, indicating that many manufacturing and production organisations use multiple restoration methods in parallel to accelerate incident recovery. Overall, 36 per cent of manufacturing and production victims used multiple methods to restore their data.

QUICK RECOVERY

Survey results showed that the manufacturing and production sector is quick to recover from a ransomware attack, with two-thirds of victims (67 per cent) getting back up and running within a week. This is considerably higher than the global cross-sector average (53 per cent), indicating that manufacturing and production is well-placed to recover from attacks.

Further demonstrating this point, just 10 per cent in manufacturing and production said it took them between one and six months to recover, compared to the global average of 20 per cent who recovered within this time.

Following the global trend across multiple industries, manufacturing and production companies have seen a decrease in the average cost to rectify the impact of the most recent ransomware attacks – from $1.52 million in 2020 to $1.23 in 2021.

Still, Sophos said $1.23 million is still a very large sum that likely has a material impact on SMB organisations in any sector.

"At first sight, it may seem counter-intuitive that the average recovery bill is less than the average ransom payment. However, in many cases, insurance providers cover ransom payments," the report stated.

There are several factors likely contributing to the below-average recovery bills for manufacturing and production.

First is the lower-than-average impact of ransomware on the operations and revenue of this sector. Secondly, the sector's impressive ability to stop the attacks before data is encrypted helps keep remediation costs low. Finally, manufacturing and production reported the highest insurance payout rate for certain costs associated with attacks (costs of downtime and lost opportunities, etc.) which likely had a commensurate impact on the total recovery costs for this sector.

CYBER INSURANCE

Many manufacturing and production organisations are choosing to reduce the risks associated with ransomware attacks by taking out cyber insurance coverage. For them, it's reassuring to know that insurers pay some costs in almost all claims.

However, only 75 per cent of manufacturing and production respondents reported having coverage against ransomware attacks, compared with a cross-sector average of 83 per cent.

Furthermore, as the cyber insurance market hardens and it becomes more challenging to secure coverage, 97 per cent of manufacturing and production organisations that have cyber insurance have amended their cyber defense to improve their cyber insurance position:

70 per cent have implemented new technologies/services – highest across all sectors.

63 per cent have increased staff training/education activities – highest across all sectors.

59 per cent have changed processes/behaviours.

"It is heartening to know that the sector leads the way in terms of implementing new technologies and services and increasing staff training," the report said. ■

FIVE TOP TIPS

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

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

Top 10 cybersecurity predictions for 2023

BeyondTrust experts forecast future threat vectors most likely to affect organizations worldwide in the New Year include a rise in ransom-vaporware, cyber un-insurability, compliance conflicts, cloud camouflage, and more

Brian Chappell, Chief Security Strategist, EMEA/APAC, BeyondTrust

As we head into 2023, the annual trends prediction season is upon us once again. BeyondTrust, a global leader in intelligent identity and access security, released its annual forecast of cybersecurity trends emerging for the New Year and beyond. These projections, authored by BeyondTrust experts Morey J Haber, Chief Security Officer and Brian Chappell, Chief Security Strategist, EMEA/APAC, are based on shifts in technology, threat actor habits, culture, and decades of combined experience.

"The Arab Gulf region continues to innovate at scale," said Morey Haber, Chief Security Officer, BeyondTrust. "But digital transformation in the cloud brings with it a range of issues, including the increased sophistication of attackers and their ability to adapt to the moment at a pace that, as yet, enterprise security functions have been unable to match."

Morey Haber, Chief Security Officer, BeyondTrust

"Our assessments of the year ahead may seem all doom and gloom, but in truth, organizations have many ways of protecting themselves against an incident," said Haber. "With the right blend of skills, tools and strategy — either in house or in collaboration with a trusted partner — businesses can go into 2023 with their eyes open and conduct their affairs with confidence," he added.

Here are the top 10 cybersecurity predictions for 2023:

Prediction #1: Negative, Zero, and Positive Trust. Next year, expect products to actually be "zero trust-ready", satisfy all seven tenants of the NIST 800-207 model, and support an architecture referenced by NIST 1800-35b. Zero trust product vendors will create marketing messages that may imply positive and/or negative intent. Some will provide positive zero trust authentication and behavioral monitoring, while others will work using a closed security model to demonstrate what should happen when a negative zero trust event occurs.

Prediction #2: Reputation for Ransom. The rise of Ransom-Vaporware. We will see a rise in the extortion of monies based

>>

>>
purely on the threat of publicizing a fictional breach. Society so willingly accepts the veracity of breaches reported in the news – and without evidence. For a threat actor, this could mean the need to perpetrate an actual breach is reduced and a threat alone, that is not even verifiable, becomes an attack vector all in itself.

Prediction #3: The Foundation of Multi-Factor Authentication (MFA) Invincibility Fails. Expect a new round of attack vectors that target and successfully bypass multifactor authentication strategies. In the next year, push notifications, and other techniques for MFA will be exploited, just like SMS. Organizations should expect to see the foundation of MFA eroded by exploit techniques that compromise MFA integrity and require a push to MFA solutions that use biometrics or FIDO2-compliant technologies.

Prediction #4: Cyber Un-insurability is the New Normal. In 2023, more businesses will face the stark realization that they are not cyber-insurable. As of the second quarter of 2022, US cyber-insurance prices already increased 79% over the prior year. The truth is, it's becoming downright difficult to obtain quality cyber insurance at a reasonable rate.

Digital transformation in the cloud brings with it a range of issues

Prediction #5: Compliance Conflicts are Brewing. Significant compliance standards, best practices, and even security frameworks, are starting to see a diverging in requirements. In 2023, expect more regulatory compliance conflicts, especially for organizations embracing modern technology, zero trust, and digital transformation initiatives.

Prediction #6: The Death of the Personal Password. The growth of non-password-based primary authentication will finally spell the end of the personal password. More applications, not just the operating system itself, will start using advanced non-password technologies, such as biometrics, either to authenticate directly or leverage biometric technology, like Microsoft Hello or Apple FaceID or TouchID, to authorize access.

Prediction #7: Cloud Camouflage is confronted. To mitigate cloud security risks, expect a push for transparency and visibility into the security operations of SaaS solutions, cloud providers and their services. The push to ensure transparency of the architecture, foundational components, and even discovered vulnerabilities, will extend beyond SOC and ISO certifications.

Prediction #8: Social Engineering in the Cloud. Attackers will turn from their software toolkits to their powers of persuasion as they increase the number of social engineering attacks leveled at employers and organizations across the cloud.

Prediction #9: Unfederated Identities to Infinity and Beyond. Expect a push into unfederated identities to help provide a new level of services and potentially physical products that will become a mild access control and management nightmare. The size and scope will feel truly infinite — unless it is well-defined for identity management teams to provide access beyond what typically is available today.

Prediction #10: OT Gets Smarter, Converges with IT. Expect attack vectors for basic Operational Technology (OT) to expand based on similar exploits that target IT. OT which once had a single function and purpose is now becoming smarter, leveraging commercial operating systems and applications to perform expanded missions. As these devices expand in scope, their design is susceptible to vulnerabilities and exploitation. ■

Wedge Networks to participate in the upcoming AICS

WEDGE Networks, an innovation leader in intelligent real-time threat prevention solutions, is participating as a silver sponsor and exhibitor in the upcoming Arab International Cybersecurity Summit (AICS) on December 6 to 8, at Exhibition World Bahrain.

A portfolio company of Bahrain-based international investment consultancy firm, Seaspring, Wedge is headquartered in Calgary, Canada with international teams in North America, Asia Pacific, Europe, and the Middle East and North Africa (Mena) regions.

A cybersecurity software vendor specialising in Real-Time Threat Prevention, Wedge Networks' WedgeARP suite (Wedge Absolute Real-Time Protection) provides highly evolved and innovative, AI-driven security protection to millions of connected systems in over 25 countries and regions.

"Wedge is committed to helping secure the cloud-connected world with global partners and various deployment options," says the company.

Wedge Networks will exhibit at the AICS summit to provide onsite live demos and exchange knowledge and ideas with industry peers.

In addition, Dr Hongwen Zhang, CEO & CTO of Wedge, will present on the importance and best practices of real-time threat prevention to secure the safety of governments, citizens and infrastructure on December 7.

As a co-founder of Wedge Networks, Dr Zhang has led the design, implementation, and launch of the firm's patented, award-winning Deep Content Inspection and Security Services Orchestration platform.

Wedge Networks will be at booth: 6-T08 ■