JAN - MAR 2023

SECURITY SOLUTIONS TODAY

DIGITAL TRANSFORMATION IN PHYSICAL SECURITY INDUSTRY

IN THIS ISSUE

CONTACT

ASSOCIATE PUBLISHER Eric Ooi (eric.ooi@tradelinkmedia.com.sg)

EDITOR Navkiran Kaur (sst@tradelinkmedia.com.sg)

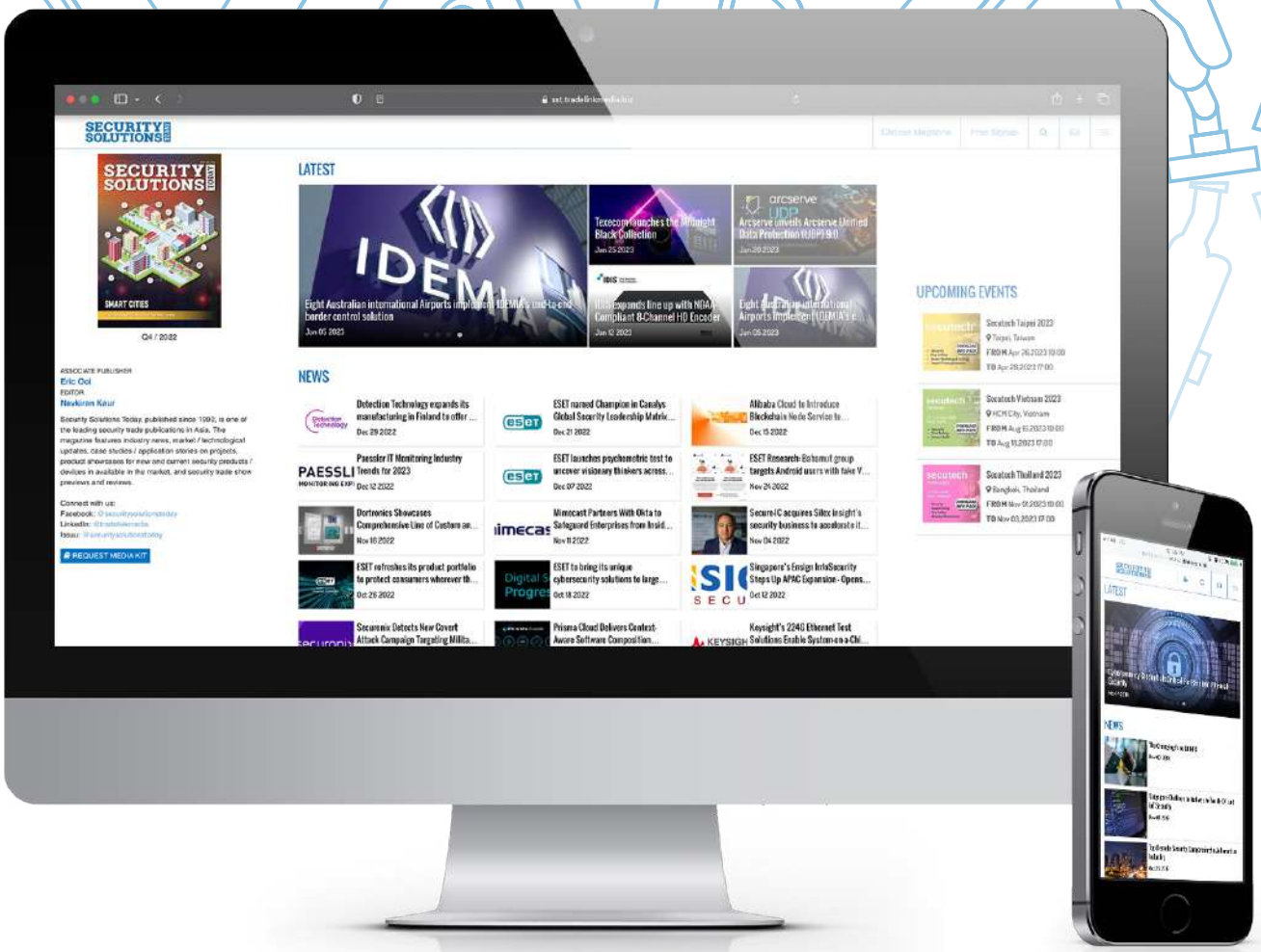
MARKETING MANAGER Felix Ooi (felix.ooi@tradelinkmedia.com.sg)

HEAD OF GRAPHIC DEPT / ADVERTISEMENT CO-ORDINATOR
Fawzeeah Yamin (fawzeeah@tradelinkmedia.com.sg)

CIRCULATION Yvonne Ooi (yvonne.ooi@tradelinkmedia.com.sg)

Vectors/Images Credit: Freepik.com
Designed by Fawzeeah Yamin

SECURITY SOLUTIONS TODAY
is published quarterly by Trade Link Media Pte Ltd (Co. Reg. No.: 199204277K)
101 Lorong 23, Geylang, #06-04, Prosper House, Singapore 388399
Tel: +65 6842 2580
ISSN 2345-7112 (E-periodical)



sst.tradelinkmedia.biz

Visit our website for the latest information

News In The Industry · Upcoming Exhibitions · Download Magazine Issues

ARMIS STATE OF CYBERWARFARE AND TRENDS REPORT: 2022-2023 HIGHLIGHTS SINGAPORE IT AND SECURITY PROFESSIONALS' SENTIMENT ON CYBERWARFARE

Singapore firms surveyed amongst the top three most likely in the world to have stalled or stopped digital transformation projects due to the threat of cyberwarfare

SINGAPORE – Armis, the leading asset visibility, and security company, today announced preliminary findings from the Armis State of Cyberwarfare and Trends Report: 2022-2023, which highlights global IT and security professionals' sentiment on cyber warfare. The study shares responses from more than 6,000 respondents across multiple industries, including 501 professionals from Singapore.

The Russian invasion of Ukraine has not only tragically upended the lives of countless people in a sovereign nation but is also causing geopolitical shockwaves of cyberwarfare that will reverberate for the foreseeable future. Today's targets extend well beyond governments; any organization is a potential victim, with critical infrastructure and high-value entities at the top of the list.

"Cyberwarfare is the future of terrorism on steroids, providing a cost-effective and asymmetric method of attack, which requires constant vigilance and expenditure to defend against," said Nadir Izrael, CTO, and Co-founder at Armis. "Clandestine cyberwarfare is rapidly becoming a thing of the past. We now see brazen cyberattacks by nation-states, often with the intent to gather intelligence, disrupt operations, or outright destroy data. Based on these trends, all organizations should consider themselves possible targets for cyberwarfare attacks and secure their assets accordingly."

"Singapore is known worldwide as a technology and innovation hub, but our survey suggests this status is under threat. Results confirm that cyber warfare is stalling or even stopping digital transformation projects across the city-state, and threat activity is on the rise," said Gwen Lee, Regional Director ASEAN, Armis. "To change this situation, organizations need to take a strategic view of cyberwarfare and secure their assets accordingly, allowing them to refocus on growing their businesses."

Key findings from the Armis State of Cyberwarfare and Trends Report: 2022-2023 include:

- Sixty-three percent of Singaporean respondents agreed that their firm had stalled or stopped digital transformation projects due to the threat of cyberwarfare, putting the city-state amongst the 3 most likely in the world to have those projects affected.
- Three in five (60%) IT and security professionals surveyed in Singapore have experienced a cybersecurity breach at their company.
- Thirty-six percent of local respondents indicated they've experienced more threat activity on their networks between May and October 2022 when compared to the six months prior. Healthcare and telecommunications firms have seen the highest increase.
- A large majority of Singapore respondents (83%) believe their companies have allocated sufficient budgets for cybersecurity programs, people, and processes.

For further information on the Armis State of Cyberwarfare and Trends Report: 2022-2023, visit: https://www.armis.com/cyberwarfare/

Methodology

Armis surveyed 6,021 IT and security professionals in firms with more than one hundred employees across the UK, USA, Spain, Portugal, France, Italy, Germany, Austria, Switzerland, Australia, Singapore, Japan, the Netherlands, and Denmark. Those findings were gathered between September 22, 2022 and October 5, 2022, and depict the state of cyberwarfare globally across various regions and industries, including financial services, healthcare, critical infrastructure, retail, supply chain and logistics, and more. From the APJ region, Armis surveyed 511 individuals in Australia, 501 in Japan, and 501 in Singapore.

About Armis

Armis, the leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust our real-time and continuous protection to see with full context all managed, unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company headquartered in California.

For more information, please e-mail:claire.wong@artemisassociates.com or dan.bradley@artemisassociates.com ■

continue on page 6

MAKE ROOM!

NOW... MORE CHANNELS OF POWER DISTRIBUTION – by ALTRONIX

Introducing **ACMS12(CB)** 12-Output Access Power Controllers with Fire Alarm Interface, and **PDS16(CB)** 16-Output Power Distribution Modules.

These new stackable sub-assemblies further increase access control capacity when integrated with Altronix Trove Series or virtually any wall/rack mount application - reducing overall equipment and installation costs.

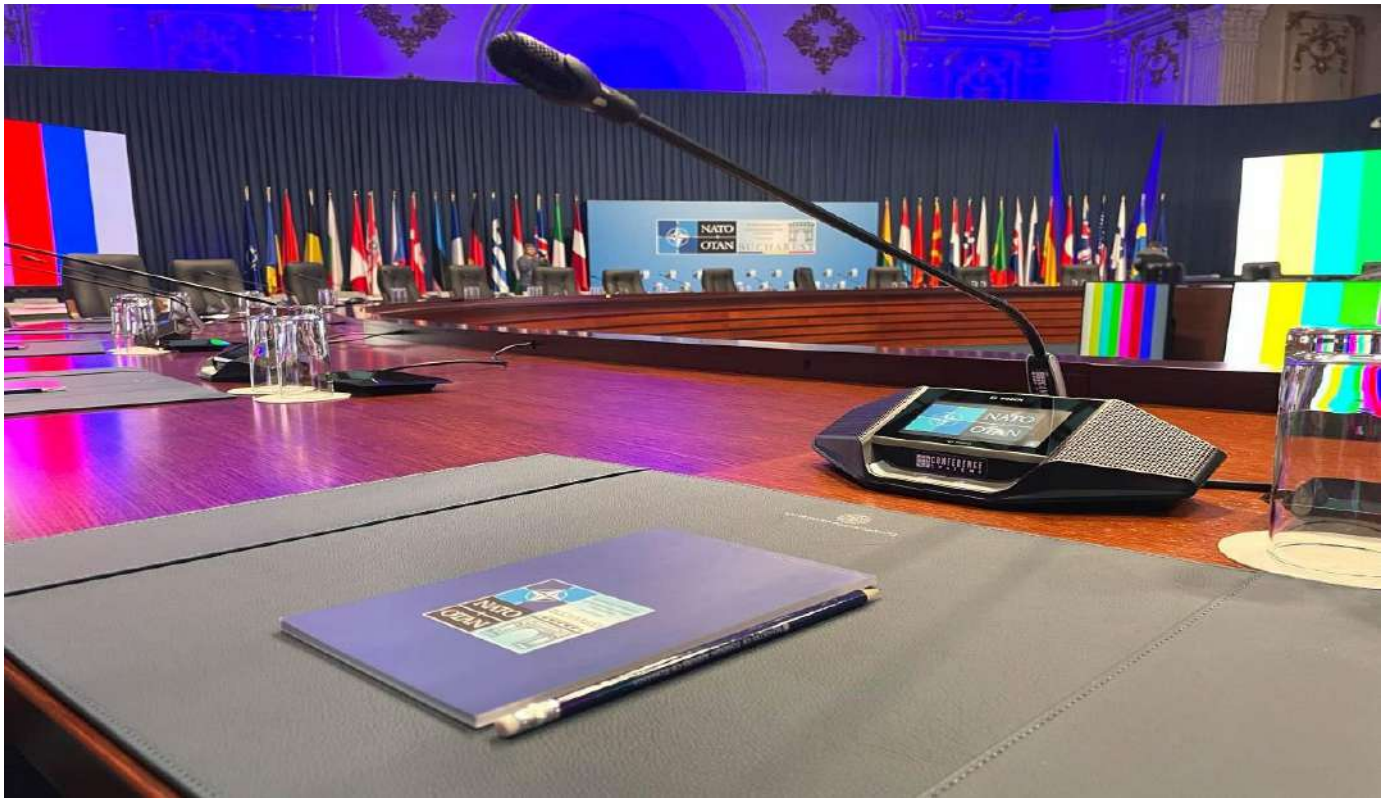
Both feature dual inputs providing selectable 12 or 24VDC from any output with bi-color voltage LEDs for visual identification.

Altronix®

YOUR LEADER IN POWER | BACKED BY A LIFETIME WARRANTY

DICENTIS CONFERENCE SYSTEM FROM BOSCH FACILITATES TOP-LEVEL MEETINGS IN EUROPE

Innovations unveiled deliver on the OpenText commitment to elevating every person and organization to gain the information advantage



The officials of the G7 Leaders' Summit and the NATO Foreign Ministers meeting in Romania at the end of 2022 both relied on Dicentis from Bosch to provide clear communications in multiple languages. With a fully IP-based architecture,

Dicentis is built on open standards to enable the highest degree of flexibility, superior audio performance for up to 100 languages, and the most powerful security protection on the market to safeguard sensitive data throughout the conference chain. The meetings both had a requirement for ISO 20109 equipment to ensure seamless and reliable operation. This made Dicentis the obvious choice for Romanian Congress Rental Network partner Conference Systems, who supplied the equipment at both events.

Encouraging Debate

While the agendas and locations for the two meetings were different, their conferencing needs were similar. As such, the Dicentis discussion device with touchscreen was the main component of both systems. Featuring a 4.3" capacitive touch screen and built-in NFC reader for fast recognition of participants, the devices are configurable for single participants, dual-users, or a chairperson, making them a flexible solution that was ideal to address the needs of both events.

"All the discussion devices were programmed in dual-use mode with the same camera prepositioning," explains Conference Systems General Manager Dan Pascu. "Camera control was done by our partner using a third-party system. We had to be sure that the system would switch every time, with the right camera and the right preposition. Both systems worked in tandem without any issues."

Dicentis interpreter desks with interpreter headphones were used for the simultaneous translations, which were distributed to participants via Integrus radiators.

The largest issue faced by the Conference Systems team came from a late change at the Romanian NATO

continue on page 7

conference. "The biggest challenge was the fact that we had to connect two booths that had been located in another area of the Romanian Parliament," recalls Pascu.

"This transformed the original setup from 10 booths plus the original language in one room to 10 booths plus two further booths in a side room, plus the original language with all the functions for the remote interpreter desk enabled." Conference Systems found out about this change just five days before the event. But thanks to the high flexibility of Dicentis and the company's deep understanding of the technology, the event passed flawlessly.

"These were both great events for us and for our partners, and we are pleased to have exceeded the clients' expectations," reflects Pascu. "As CRN representative for Romania, we have once again proved the quality of the services provided by any CRN member on five continents when we rely on Dicentis."

For more information, please e-mail: florian.lauw@de.bosch.com ■

C3 AI ANNOUNCES LAUNCH OF C3 GENERATIVE AI PRODUCT SUITE

General availability March 2023

C3 AI (NYSE: AI), the Enterprise AI application software company, today announced the launch of the C3 Generative AI Product Suite with the release of its first product — C3 Generative AI for Enterprise.

C3 Generative AI for Enterprise Search provides enterprise users with a transformative user experience using a natural language interface to rapidly locate, retrieve, and present all relevant data across the entire corpus of an enterprise's information systems.

The C3 Generative AI Product Suite integrates the latest AI capabilities from organizations such as Open AI, Google, and academia, and the most advanced models, such as ChatGPT and GPT-3 into C3 AI's enterprise AI products.2

"C3 Generative AI fundamentally changes the human computer interaction model of enterprise application software," said C3 AI CEO Thomas M. Siebel. "Combining the full potential of natural language, generative pre-trained transformers, enterprise AI, and predictive analytics will change everything about enterprise computing."

Image by rawpixel.com on Freepik

The C3 Generative AI Product Suite embeds advanced transformer models with C3 AI's pre-built AI applications accelerating customers' ability to leverage these models across their value chains. C3 Generative AI will accelerate transformation efforts across business functions and industries, including supply chain, sustainability, reliability, CRM, ESG, aerospace, oil & gas, utilities, CPG, healthcare, financial services, and defense and intelligence.

"This is game changing for U.S. DoD, game changing for the U.S. intelligence community, and game changing for ubiquitous information access and insight," said Lt. Gen. Ed Cardon (Ret.), former commanding general of the U.S. Army Cyber Command. "This technology breakthrough can help dissolve the biggest barrier that we have to effective action, which is access to timely, accurate information and insight at all levels of the organization."

C3 Generative AI is scheduled for general release in March 2023 and will be featured at the C3 Transform international users' group conference in Boca Raton, FL, on March 7, 2023.

About C3.ai, Inc.

C3 AI is an Enterprise AI application software company. C3 AI delivers a family of fully integrated products, including the C3 AI Platform, an end-to-end platform for developing, deploying, and operating enterprise AI applications, C3 AI applications, a portfolio of industry-specific SaaS enterprise AI applications that enable the digital transformation of organizations globally, and C3 Generative AI, a suite of large AI transformer models for the enterprise.

For more information, please e-mail: pr@c3.ai ■

DIGICERT INTRODUCES DIGICERT® TRUST LIFECYCLE MANAGER, SETS A NEW BAR FOR UNIFIED MANAGEMENT OF DIGITAL TRUST

Full-stack solution unifies CA-agnostic certificate management, private PKI services, and public trust issuance for seamless digital trust infrastructure

DigiCert, Inc., a leading global provider of digital trust, today announced the release of DigiCert® Trust Lifecycle Manager, a comprehensive digital trust solution unifying CA-agnostic certificate management and public key infrastructure (PKI) services. Trust Lifecycle Manager tightly integrates with DigiCert's best-in-class public trust issuance for a full-stack solution governing the seamless management of corporate digital trust infrastructure.

Organisations that prioritize a unified digital trust strategy add to their top line and protect their bottom line. At the top line, digital trust accelerates customer acquisition, improves employee productivity, and drives digital innovation. At the bottom line, it reduces the risk of outages of mission-critical applications, the attack surface area for breaches, and customer churn due to loss of trust. The 2022 State of Digital Trust Survey revealed the cost of poor security practices, finding that almost half of the consumers have stopped doing business with a company after losing confidence in its digital trust competency.

"In an always-on, digitally connected world, to ensure digital trust, connections cannot be disrupted, terminated or altered without consequence," said Jennifer Glenn, Research Director for IDC. "Centralizing certificate management improves visibility into the certificate landscape and provides a basis for automation, which is instrumental in keeping business systems connected and running securely and efficiently."

Added Deepika Chauhan, DigiCert's Chief Product Officer, "DigiCert Trust Lifecycle Manager is setting a new standard for managing trust within an organization's ever-expanding digital footprint. Customers can centralize management of their entire digital certificate and PKI assets in a unified, flexible architecture that seamlessly integrates with existing business processes and systems."

Trust Lifecycle Manager brings together:

- Certificate lifecycle management, streamlining IT operations with certificate discovery, management, notification, automation, and integration.
- PKI services, streamlining identity and authentication with private certificate issuance for users, devices, servers, and other IT resources, and management of the CA hierarchy.

This unified management of a company's digital trust fabric delivers:

- A full-stack solution in a single pane of glass that offers superior performance, handling, and automation, with single-vendor accountability.
- Certificate profiles and tools facilitating self-service issuance.
- Flexibility for cloud, on-premises, or hybrid models, enabling companies to manage their PKI use cases according to their security policy preferences.
- Centralized visibility and control over a company's certificate landscape, reducing the risk of business disruption and securing identity and access across the organization.
- Deep integration into user and enterprise technologies, supporting existing business systems and processes.

Trust Lifecycle Manager is generally available now as part of the DigiCert® ONE platform. To learn more, visit www.digicert.com/trust-lifecycle-manager, and register here to join a launch event on Feb. 1.

About DigiCert, Inc.

DigiCert is a leading global provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert® ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access, and communication, software, identity, content, and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support, and operations and is the digital trust provider of choice for leading companies around the world.

For more information, visit www.digicert.com or follow @digicert. ■

LG SHOWCASES ITS LATEST DISPLAY SOLUTIONS UNDER THE THEME OF "LIFE, BE BLOOMED" AT ISE 2023

LG's Advanced Display Innovations, including 8K Micro LED, Feature an Interactive Exhibit Along with Immersive Media Art and Digitalized Spaces for Diverse Industries

LG Electronics (LG) is presenting its cutting-edge digital signage solutions at Integrated Systems Europe (ISE) 2023, which will be held in Barcelona, Spain, today. The company's full range of display solutions – including Micro LED displays, Transparent OLED Signage, and LED displays – is exhibited across a number of digitalised spaces demonstrating use cases and applications for different industries, including retail, corporate, education, and hospitality.

Adopting the theme of Life, Be Bloomed for this year's ISE, LG is presenting innovative display solutions that offer a world of possibilities and the power to make life better, each and every day. Visitors to the company's booth will be able to experience solutions created to foster better business communications, solutions that deliver clear visibility and integrate seamlessly into various commercial environments and solutions that can convey the emotion and dynamism of stunning digital artworks in a whole new way.

The massive 272-inch LG MAGNIT 8K Micro LED (LSAB007) is making its debut at ISE with a truly jaw-dropping display – both in scale and in picture quality. The enormous Micro LED leverages millions of self-emissive micrometre-scale pixels to create images of exceptional vibrancy and depth, while its 8K resolution (7,680 x 4,320) delivers razor-sharp detail.

LG MAGNIT 8K offers impressive colour consistency and a wide viewing angle. This remarkable display solution will mesmerise visitors to the company's booth, enthralling them with exclusive 8K footage that captures the beauty and majesty of the natural world. With its huge size and superb picture quality, LG MAGNIT is an excellent solution for showcasing media art in public spaces and for use in building control rooms, boardrooms, and corporate and hotel lobbies.

Another spectacular sight for visitors, LG's 8K Micro LED synchronises with 56 Transparent OLED Signage (55EW5G-V) displays covering both sides of the LG exhibition hall's entrance to create an incredibly immersive media art experience. The captivating display setup transports visitors into a world of colour and wonder – a world brought to life by the company's cutting-edge display technologies.

At ISE 2023, LG is also showcasing its solutions for virtual production studios for the very first time. A virtual production studio allows content creators to shoot live-action footage against a fully digital backdrop, which is made by displaying virtual scenery on a series of seamlessly connected LED screens. LG and its professional partners, including Mo-Sys and ARRI will be showing visitors how a virtual production studio works – and how it can be used for entertainment applications, such as film and TV, and for corporate in-house broadcasting – and introducing LG's LED displays and related solutions.

At the center of LG's booth is the eye-catching Floating CUBE LED, an LED sculpture that creatively combines four 2K LED displays (LSCB012). Based on Tensegrity, a structural principle of tensional integrity, the CUBE presents strikingly three-dimensional anamorphic digital art that moves and flows across the displays' surfaces. LG's fine-pitch LED displays provide lifelike picture quality, while the seamless 90-degree corner design of the CUBE installation enhances the sense that one is looking at real, 3D objects inside an actual, physical space.

Additionally, LG is introducing its new digital learning solution, LG CreateBoard (TR3DK), at ISE 2023. An Interactive Digital Board designed to engage, inform, and inspire students and encourage greater collaboration, the new model provides LG CreateBoard Lab for content creating and writing, and LG CreateBoard Share for wireless content and screen sharing. Also on

continue on page 10

show is LG ConnectedCare DMS, a cloud-based device management solution for schools and other learning environments that enables the remote management of multiple displays.

As part of its comprehensive exhibit, LG is presenting convenient cloud-based management solutions tailored to the needs of diverse industries; including retail, corporate, education, and hospitality. LG Pro: Cloud is a cloud platform for accessing LG's content management solutions (CMS), including Pro: Centric Cloud (hospitality) and SuperSign Cloud, while LG ConnectedCare is a remote management solution that makes it possible to monitor signages, check energy usage and adjust display brightness via the integrated Energy Dashboard.

Also on full display at ISE 2023 is LG's ongoing commitment to sustainability. Embracing the company's 'Better Life for All' vision, the latest B2B solutions from LG offer energy efficiency, reduced resource consumption, increased recyclability, and enhanced accessibility.

In the ESG zone, visitors can explore innovations such as cloud-based smart energy management solutions that help to reduce power consumption and 4K UHD signage (UL3J-EP), featuring components partially made from recycled plastic, and check out the LG Kiosk, which promotes digital inclusion with a tactile keypad for the visually impaired.

"At ISE 2023, LG is demonstrating how its display solutions can add value in practically any commercial sector, or area of your life, you care to name," said Paik Ki-mun, senior vice president and head of the Information Display business unit of LG Electronics Business Solutions Company. "Far more than just screens for presenting content, our display solutions can help you connect, create, communicate, and collaborate – expanding and digitalising your daily experience in a host of convenient, new ways."

Visitors to ISE 2023 can find LG's booth in Hall 3 (Stand 3K 200) of Fira Barcelona's Gran Via conference center. **To learn more about LG's digital signage solutions at ISE 2023, please visit www.lg-informationdisplay.com/ise2023.**

About LG Electronics Inc.

LG Electronics, Inc. is a global innovator in technology and manufacturing, with operations in more than 100 locations around the world. With 2017 global sales of USD 55.4 billion (KRW 61.4 trillion), LG is comprised of five companies— Home Appliance & Air Solutions, Home Entertainment, Mobile Communications, Vehicle Components, and Business-to-Business — and is a world-leading producer of TVs, refrigerators, air conditioners, washing machines, and mobile devices in addition to premium LG SIGNATURE products and ThinQ featuring artificial intelligence.

About LG Electronics Business Solutions Company

The LG Business Solutions Company is a trusted partner offering innovative products and solutions for diverse industries worldwide. With a portfolio of unique offerings, such as industry-leading OLED and LED signage, LG is a respected name among customers around the world. LG's IT solutions include business monitors, laptops, projectors, cloud devices, medical displays, and commercial robots, all designed to maximize work efficiency and return strong value to customers. **For more on LG's Business Solutions, visit www.LG.com/b2b.**

About LG Electronics Singapore Pte Ltd

LG Electronics Singapore Pte Ltd (LG Electronics Singapore) is a fully-owned subsidiary of LG Electronics Inc., the pioneer and market leader of the Korean electronics industry. LG Electronics Singapore operates four business units locally – Home Entertainment, Home Appliance, Air Solutions, and Business Solutions. In recognition of its vision to enrich people's life with smart technologies and innovative design, LG Electronics Singapore has been recognized with prominent local and international accolades, such as the CNET Asia Editor's and Readers' Choice Awards, HWM+HardwareZone.com Tech Awards, Red Dot Design, and GfK No. 1 Awards. **For more information, please visit www.lg.com/sg.** ■

GENZNOMICS: 10 GENZ BELIEFS & BEHAVIORS DRIVING THE GLOBAL ECONOMY

As a GenZ authority and policy advocate, I believe it is essential to advance a cross-generational understanding of the driving forces behind the post-millennial economy in order for the industry to establish best practices and move forward in a meaningful and impactful way. GenZ, the "iGen" demographic cohort born between 1997 and 2012, is the first to grow up fully immersed in technology. As such, we "Zoomers" is known for a high level of digital savviness that has underpinned their unprecedented entrepreneurial spirit—and their abrogation from societal norms.

continue on page 11

Image by Freepik

While there are a myriad of behaviors and beliefs that heavily influenced GenZ's economic decisions, there are a select group of specifics that reign supreme—especially with respect to these four economic sectors:

- **Artificial Intelligence (AI) Industry:** GenZ is highly interested in the AI industry and its potential to revolutionize various sectors, such as healthcare, education, and transportation. According to a survey by Deloitte, 51% of GenZ respondents said they are interested in a career in technology; this includes degrees in computer and information sciences rising 38% from 2015 - 2019. Furthermore, a report by the World Economic Forum predicts that AI will create 58 million new jobs by 2023. GenZ is well-positioned to take advantage of these opportunities and shape the future of the AI industry.

- **Web3 Industry:** GenZ has a strong interest in the Web3 industry, which includes decentralized technologies such as blockchain, cryptocurrency, and smart contracts. They see the potential of Web3 to create a more decentralized and transparent internet, where data is controlled by the users instead of a handful of big tech giants. According to a survey by Chainalysis, 64% of GenZ respondents said they own or have owned cryptocurrency, compared to only 22% of millennials. Furthermore, a report by Gartner predicts that by 2025, the business value added by blockchain will reach $3.1 trillion. GenZ is poised to play a vital role in shaping the future of the Web3 industry.

- **Natural Resource Energy Economy:** GenZ cares deeply about the environment and the impact of human activities on climate change. They understand the need to transition to a more sustainable energy economy that is based on renewable resources. According to a survey by the Pew Research Center, 6 9% of GenZ respondents said they are worried about climate change, compared to 59% of millennials. Furthermore, a report by the International Energy Agency predicts that renewable energy sources could account for 9 0% of the world's power generation by 2050. GenZ is well-positioned to lead the transition to a more sustainable energy economy.

- **Social Media Economy:** GenZ is highly active on social media and is well-versed in the workings of the social media economy. They understand the power of influencer marketing and the role of these platforms in shaping public opinion. According to research, GenZ is 59% more likely to connect with brands online than other generations. Furthermore, a report by Business Insider predicts that the global influencer marketing industry will be worth $15 billion by 2023. GenZ is poised to shape the future of the social media economy through its participation as influencers and consumers.

Mindsets Matter: Key Factors Driving GenZ Beliefs and Behaviors

As Gen Z belief systems and behaviors are a driving force not only in shaping culture but economies at the global level, it's imperative to understand commonalities in order to discern opportunities and challenges that lie ahead. Here are my top 10.

continue on page 12

Consumerism and Motivation to Succeed: Many Gen Z prioritizes their career and financial goals over immediate gratification in their personal lives. They are more materialistic and motivated to succeed than previous generations, with an overall goal of achieving financial security and an upper-middle-class lifestyle that now is seemingly out of reach for many as wages remain stagnant over time. According to a survey by Bank of America, 45% of GenZ respondents said that material goods are a major priority for them, compared to only 34% of millennials.

Slow Living: GenZ values a slower pace of life and is more focused on living in the present moment. According to a study by EY, 67% of GenZ is moderately to extremely worried about their physical and mental health, making health a high priority for this generation. They also distinguish between "quiet quitting," which many in the generation believe is simply giving only as much into their job as their job compensates them for vs Slow Living, which involves setting healthy boundaries between work and personal life.

Emphasis on Multiple Income Streams: GenZ is more likely to have multiple streams of income, such as a part-time job, freelancing, or a side hustle. They understand the importance of diversifying their income sources to mitigate financial risk and also see additional streams of income as a necessity in an economy of stagnant wages. A survey by Lending Tree found that 62% of GenZ respondents have a side hustle as compared to 55% of millennials.

Budgeting and Understanding Credit: GenZ is known for its budgeting skills and understanding of credit. After watching their parents face the consequences of the 2008 financial crisis, they tend to be more financially savvy and responsible than previous generations. According to Finder's Consumer Confidence Index, Gen Z saves an average of $857 a month, while Millennials save $294.

Trade School and Specialization: GenZ values practical skills and specialized knowledge. They are more willing to pursue trade schools or specialized degrees that offer a clear career path and high earning potential. They also tend to be more cost-conscious and are willing to weigh the cost-benefit of higher education, given the skyrocketing cost of higher education and the known risks of student debt. NPR reports that while enrollment in community colleges is down, trade schools have seen enrollment numbers increase in recent years.

Technological Proficiency: GenZ is the first generation to grow up fully immersed in technology. They are more comfortable with technology and are more likely to pursue careers in the tech industry. They are also more efficient in their work. A report by Under Cover Recruiter references Gen Z as "skilled when it comes to technology savants, online work, and innovation."

Retirement: GenZ is less concerned with retirement than previous generations. They tend to prioritize their current financial and career goals over planning for their retirement. A survey by antyimesestimate.com found that GenZ makes up the largest group of Americans (44%) not saving for retirement.

Employer Loyalty: GenZ values loyalty from their employers. They understand that loyalty is not inherent and must be earned through mutual respect and appreciation. They also prioritize feeling appreciated and acknowledged in their work over staying with a company long-term. A survey by PromoLeaf found that Gen Z respondents want to spend an average of 3.7 years on a job.

Parental Trust: GenZ is more trusting of their parents than millennials when it comes to financial advice. A survey by YPulse found that 70% of GenZ respondents said they usually or always trust their parents to give them good financial advice, compared to only 60% of millennials. This trust in their parents can be attributed to the fact that GenZ has grown up during a time of economic uncertainty and has seen their parents navigate through financial challenges. They see their parents as a reliable source of financial guidance and advice. This may be a reflection of the increased transparency and engagement Gen X parents offered their children in comparison to previous parental generations.

Home Ownership: GenZ does not see home ownership as a priority, or even an attainable goal, as previous generations did. According to a recent article by Levi Leidy, while Millennials lag behind Gen X, Baby Boomers, and Silent Generation in homeownership at age 40, the trend is expected to continue with Gen Z, and they are aware of it. The high cost of housing and student loan debt are among the reasons that make it difficult for GenZ to afford a home. Additionally, many GenZ has seen their parents struggle with mortgages and foreclosures during the 2008 financial crisis, which has made them more cautious and hesitant about buying a home.

In spite of their widely-reported worries, a McKinsey & Company study denotes optimism among Zoomers. "GenZ thinks the economic future is brighter than most other age groups do," the report cites. "Despite reporting higher levels of job insecurity and financial instability and higher rates of emotional distress and obstacles to working effectively, GenZ's view of economic opportunity is more optimistic than that of GenX and baby boomers."

Reputed for being "highly collaborative, self-reliant and pragmatic," GenZ just might be the lot to live out this ubiquitous American dream if the industry collectively adapts to even just these 10 specific proficiencies, inclinations, and expectations.

continue on page 13

Cheyenne Hunt, J.D. is a progressive advocate and attorney specializing in progressive activism, legislative advocacy, communications, and democracy-focused tech policy. She currently serves as a Big Tech Accountability Advocate with Public Citizen. She graduated from the University of California Irvine School of Law, earned Dual Degrees in Political Science and Public Policy from the University of Denver, and serves as a board member for The Women of Global Change. **Connect with her on LinkedIn at https://www.linkedin.com/in/cheyenne-hunt-7b921621b.** ■

ESET RESEARCH: RUSSIAN APT GROUPS, INCLUDING SANDWORM, CONTINUE THEIR ATTACKS AGAINST UKRAINE WITH WIPERS AND RANSOMWARE

- ESET released its latest APT Activity Report, covering the period from September until the end of December 2022 (T3 2022).
- Russia-aligned APT groups continued to be particularly involved in operations targeting Ukraine, deploying destructive wipers such as NikoWiper. Sandworm launched the wipers in parallel with Russia's armed forces launching missile strikes targeting energy infrastructure. While ESET is not able to show that those events were coordinated, it suggests that Sandworm and the military forces of Russia have related objectives.
- Russian APT groups attacked Ukraine with ransomware (Prestige, RansomBoggs).
- Along with Sandworm, other Russian APT groups, such as Callisto and Gamaredon, continued their spearphishing campaigns against the Eastern European nation.
- China-aligned groups, specifically Goblin Panda, started duplicating Mustang Panda's interest in European countries.
- Iran-aligned groups continued to operate at a high volume.

ESET Research today released its latest APT Activity Report, which summarises discoveries about select advanced persistent threat (APT) groups that were observed, investigated, and analysed by ESET researchers between September and the end of December (T3) 2022. During this period, Russia-aligned APT groups continued to be particularly involved in operations targeting Ukraine, deploying destructive wipers and ransomware. Goblin Panda, a China-aligned group, started to duplicate Mustang Panda's interest in European countries. Iran-aligned groups continued to operate at a high volume, too.

Vector by Freepik

In Ukraine, ESET detected the infamous Sandworm group using a previously unknown wiper against an energy sector company. Nation-state or state-sponsored actors usually operate APT groups; the described attack happened in October during the same period when Russian armed forces began launching missile strikes targeting energy infrastructure. While ESET is not able to show that those events were coordinated, it suggests that Sandworm and the Russian military have related objectives.

ESET has named the latest wiper from a series of previously discovered wipers, NikoWiper. This wiper was used against a company in the energy sector in Ukraine in October 2022. NikoWiper is based on SDelete, a command line utility from Microsoft that is used for securely deleting files.

In addition to data-wiping malware, ESET discovered Sandworm attacks using ransomware as a wiper. In those attacks, although ransomware was used, the final objective was the same as for the wipers: data destruction. Unlike traditional ransomware attacks, the Sandworm operators do not intend to provide a decryption key.

In October 2022, ESET detected Prestige ransomware being deployed against logistics companies in Ukraine and Poland. And in November 2022, ESET discovered new ransomware in Ukraine written in .NET that we named

continue on page 14

RansomBoggs. ESET Research publicly reported this campaign on its Twitter account. Along with Sandworm, other Russian APT groups such as Callisto and Gamaredon have continued their spearphishing campaigns against Ukraine to steal credentials and install implants.

ESET researchers also detected a MirrorFace spearphishing campaign targeting political entities in Japan and noticed a gradual change in the targeting of some China-aligned groups – Goblin Panda started to duplicate Mustang Panda's interest in European countries. Last November, ESET discovered a new Goblin Panda backdoor, which we named TurboSlate, in a government organisation in the European Union. Mustang Panda has also continued to target European organisations. Last September, we detected a Korplug loader used by Mustang Panda at an organisation in Switzerland's energy and engineering sector.

Iran-aligned groups continued their attacks, too – besides Israeli companies, POLONIUM also started targeting the foreign subsidiaries of Israeli companies, and MuddyWater probably compromised a managed security service provider.

North Korea-aligned groups used old exploits to compromise cryptocurrency firms and exchanges in various parts of the world. Interestingly, Konni has expanded the repertoire of languages it uses in its decoy documents to include English, which means it might not be aiming at its usual Russian and South Korean targets.

For more technical information, check the full "ESET APT Activity Report" on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real-time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future.

For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter. ■

GJD ANNOUNCES NEW UK SALES MANAGER

GJD strengthens the UK sales team with the addition of a new regional sales manager, Ben Lea.

GJD, an AVA group company and global leader in perimeter protection and illumination solutions, is pleased to announce and welcome Ben Lea as GJD's new regional sales manager for North England, Ireland, and Scotland. Ben will be the key account manager for these areas, and his responsibilities will include supporting the company's distributors, installers, and partners. Ben will also be responsible for contributing to GJD's overall success and developing the company's customer base in the UK.

Ben has many years of experience working in the security industry. Previously working as a sales engineer for one of the largest security distributors in the industry. He has also worked in the security installation sector, helping customers design solutions from initial concept to completion. Ana Maria Sagra-Smith, GJD's Sales and Marketing Director, commented: "We are pleased to announce the appointment of Ben within the UK sales team. Ben is well suited for this role, and I am confident that his wealth of sales management experience and valuable technical knowledge of the GJD product range will provide our distributors, installers, and partners with the outstanding service and support that they deserve."

Ben added: "I'm very excited to join GJD, a company with a long history of British manufacturing. I look forward to meeting my customers and providing perimeter protection solutions that best fit individual project requirements." GJD has been providing reliable detection and intelligent deterrent solutions for the global security market for nearly 40 years. Products in the GJD range identify genuine threats and create alerts when an intruder crosses the boundary rather than when it is too late and they are already inside the premises.

About GJD

GJD is an award-winning British manufacturer of external detection, LED illumination, and ANPR equipment. We design and develop reliable products that perform time after time without fail. We are committed to building and developing reliable partnerships. We are invested in creating seamless integration for the perfect user experience.

For more information about GJD, please visit www.gjd.co.uk ■

INDIA TO BECOME GLOBAL AI HUB

From automating tasks and fraud prevention to developing next-gen medical solutions, companies across sectors are riding the tailwinds of artificial intelligence (AI).

The next decade will see more tangible results over audacious AI claims. Against the backdrop, India is all set to leapfrog in AI adoption with a holistic approach supported by robust tech-driven infrastructure and strong government impetus, finds GlobalData.

Kiran Raj, Practice Head of Disruptive Tech at GlobalData, comments: "While digitalization continues to be a major cause for the sweeping transformation across sectors in India, AI will be a fundamental building block underpinning the enterprise digital infrastructure. The country seems to have all the right ingredients in place to make it big in AI, right from dominant position in IT to companies prioritizing efficiency and cost-savings by implementing a holistic approach for intelligent automation, quicker turnaround, and conflict resolution."

Shagun Sachdeva, Project Manager of Disruptive Tech at GlobalData, comments: "The COVID-19 pandemic accentuated the shift towards digitalization in a relatively short period of time. 2022 laid down the roadmap for various technology integrations, including AI, and 2023 will only take it forward. GlobalData sees more and more use cases of AI-powered technology across primary, secondary, and tertiary sectors of the Indian economy."

An analysis of GlobalData's Disruptor Intelligence Center highlights India's AI adoption in terms of startup activity and mergers & acquisitions (M&A).

According to GlobalData's Unicorn Prediction model, 28 Indian startups out of 132 AI startups in Asia-Pacific (APAC) are predicted to create massive technological disruption and have the potential to become unicorns as of December 2022. In the Indian agri sector, for instance, CropIn Technology Solutions is leveraging AI to improve the productivity and profitability of growers and food processors and allow users to capture real-time data from agricultural farms.

Sachdeva adds: "Amid the prevailing global uncertainty, startups are currently on shaky grounds with funding winter, massive layoffs, delayed IPOs, and uncertain profits; therefore, realigning goals and rethinking growth strategies is the need of the hour."

The AI M&A activity in India rose to 58 deals in 2022 from 25 in 2020, a massive rise of 132%. In December 2022, Wipro Infrastructure Engineering acquired Linecraft.ai, a Pune-based AI-enabled company that empowers manufacturers to get more productivity and quality, thus improving operational efficiency on a real-time basis.

In August 2022, Axis Bank announced to acquire 5.09% stake in CredAble, an AI-powered fintech platform that enables working capital financing across enterprise ecosystems.

In June 2022, Maruti Suzuki announced the acquisition of a 12.09% stake in Sociograph Solutions, a provider of visual AI platforms for enterprises to improve sales experiences and improve efficiency.

Sachdeva concludes: "Without a doubt, the recent developments in AI have put India on the cusp of a new automation age. The AI adoption and awareness in the country is expected to reach its pinnacle in the next five years as companies integrate AI with edge computing, Industry 4.0, and real-time analysis for complex problems." ■

MAXXESS TO HIGHLIGHT THE LATEST INTEGRATIONS AND PROJECT SUCCESSES AT INTERSEC

Landmark projects across the Middle East are taking advantage of eFusion's expanding ecosystem

Maxxess will be at Intersec showcasing the extended ecosystem of integrations now available with its eFusion access control and integrated security management platform, as well as the latest, powerful functionality available with its eVisitor visitor management solution. Visitors to Digifort stand S1-F09 will also learn about the run of recent major integration projects taking advantage of the technology, including high-end hotels, landmark mixed-use developments, and major corporate and industrial sites.

eFusion, now widely used in industrial settings, the hospitality sector, and mixed-use developments is a feature-rich platform that allows seamless off-the-shelf integration with more than 60 leading technologies. These include video surveillance, fire, and building management systems, as well as site-specific applications and hardware.

Expanding customers' choice to a wider range of VMS and camera brands managed through the eFusion interface, new integrations will include the full suite Digifort's of video management as well as the latest facial recognition technology.

Recent major projects taking advantage of eFusion's modular building block approach include the Jumeirah Al Marsa hotel and harbour development, the multi-use Wasl Tower, Bluewaters Island including the Ain in Dubai, and the Yanbu Aramco Sinopec Refinery (YasRef) in Saudi Arabia.

eFusion's transparent price structure ensures affordability but gives users a level of power and functionality previously only associated with more expensive, tailored solutions.

"By bringing together previously siloed systems, eFusion users can leverage operational efficiency by removing the need for operators to continually switch between screens and interfaces," says Lee Copland, Managing Director EMEA, Maxxess. "This allows busy operational teams and control room managers to focus on priority tasks rather than having to juggle with disparate technologies."

Meanwhile, he added that eVisitor's growing popularity is due to its successful focus on enabling frictionless and touchless access to premises, increasing efficiency and security while removing inconveniences for the visitors, staff, and contractors typically encounter when accessing car parking and facilities.

"eVisitor integrates with multiple systems and popular corporate databases, including Assa Abloy Hospitality and Microsoft Active Directory, and facilitates hassle-free time and attendance management to further eliminate the inefficiencies of siloed systems and technology stacks." To book a demo or meeting at the show, please email sales@maxxess-systems.com or go to www.maxxess-efusion.com for more information.

About Maxxess

Maxxess is a U.S.-based, privately held, global corporation specializing in security management solutions and innovative technologies that are effectively transforming the way businesses approach and implement security. Leading organisations worldwide, from healthcare to hospitality and transportation to telecommunications, choose Maxxess for the company's expertise in access control, security system management software and mobile safety applications. The company is committed to advancing open architecture software, development of leading-edge technologies, first-class customer care, plus fair, transparent pricing structures. Maxxess' systems are in use in more than 10,000 installations worldwide with clients including Emirates Airlines, Banner Healthcare, Fluor Corporation, Open University, Loyola University and CAE, as well as an additional 300 schools and universities and more than 100 hospital and healthcare facilities. Established in 2003, Maxxess has dedicated sales and technical teams in the Middle East, Europe, and North America.

For more information, please visit www.maxxess-systems.com. ■

OPEN-SOURCE INTELLIGENCE IN RUSSIAN INVASION OF UKRAINE

Flashpoint's new report on the role of open-source intelligence (OSINT) in the Russia-Ukraine war has now been released.

As Russia's full-scale invasion of Ukraine approaches the one-year mark, Flashpoint has released its report of ten real-life examples detailing how OSINT has helped organisations across the public, and private sectors understand a hybrid war that spans cyber, physical, and informational domains.

"It has become a near imperative for just about every organisation in the world, from governments to enterprises, to be able to acknowledge and calculate their risk profiles in relation to the war," said Andras Toth-Czifra, Senior Intelligence Analyst at Flashpoint. "And because we will likely still see changes in how this war is fought—by what means and at which targets—the importance of obtaining accurate, timely, and actionable intelligence remains essential."

Report highlights include:

- **Recruitment on the frontlines:** Where the convergence of cyber and physical intelligence identifies how internet-driven communication and funding influence and enable kinetic movement and warfare.
- **Cryptocurrency and illicit financing:** The intel, which triangulates blockchain and threat intelligence, provides insight into on-the-ground operations of mercenary groups and private military companies involved in the war, including troop movement, communication and transaction methods, and arms, supply, and infrastructure needs.
- **Destructive malware wipers:** This intelligence allows visibility over the tools deployed over Ukrainian and Western networks, as well as the risk of wipers being used against critical infrastructure systems in countries allied to Ukraine.
- **Killnet:** Russia's favourite DDoS hacktivist collective has conducted distributed denial-of-service attacks on entities it deems to be supportive of Ukraine. Despite Killnet's loud claims of being an ideologically motivated collective, the group still accepts commercial orders. All of those mentions of Killnet in the world's top publications have likely brought new DDoS customers to the table.

- **Battle for the Russian**-Language darknet. One of the ongoing processes that Russia's February invasion has accelerated is the fragmentation of the Russian-speaking cyber underground. This includes a rivalry that emerged over the summer between two leading competitors, RuTor/OMGOMG and WayAWay/Kraken.

- **Documenting violence:** For the duration of the war, eyewitnesses, military bloggers, correspondents, soldiers, and mercenaries alike have shared both textual information and visual media on Telegram and other platforms. These have been used as material for open-source investigations of the placement, activities, and identities of invading troops, as well as the atrocities committed by them. In future court proceedings on war crimes, this data could be crucial evidence.

- **War bloggers and policy:** Since the beginning of Russia's invasion of Ukraine, a wide range of popular, pro-Kremlin channels have emerged on Telegram, and they have come to shape the domestic image of the war. They are run by war correspondents of state-backed media, military bloggers, and mercenary groups, as well as domestic politicians and propagandists. While the narratives promoted by them have often aligned with the Kremlin's preferred narratives, at times, they have been markedly critical of Russia's leaders.

- **Iranian unmanned aerial vehicles (UAVs) bring strength to the Russian military:** The vast number of images and footage related to Iranian UAVs in use in Ukraine enabled Flashpoint users to monitor the types of UAVs in use by Russian forces; gain a clearer picture as to how these UAVs fit into Russia's war strategy; and understand how Ukrainian forces are confronting the threat.

- **Mobilisation protests in Russia:** Russian President Vladimir Putin's decree announcing a "partial" mobilisation in Russia caused an immediate response. In the following days, hundreds of thousands of Russian citizens fled abroad as draft protests started in several regions. Flashpoint observed a growing number of chatter and advertisements on Russian-language illicit communities and social media platforms, offering methods or access to avoid the draft. Furthermore, monitoring events like this helps to understand the domestic reaction of Russian society to the ongoing war and the potential impact on an internal coup in Russia.

- **Disinformation, conspiracy theories, and justification narratives:** Disinformation narratives are very closely woven into the events of this war, lasting from Russia's annexation of Crimea in 2014 to today's ongoing invasion of Ukraine. These narratives have the power to shape political and kinetic decision-making; they are also effective tools for psychological influence. ■

OTORIO RELEASES MICROSOFT DCOM HARDENING TOOLKIT FOR OT SYSTEMS

New Open Source Detection Tool Uncovers Vulnerable DCOM in Advance of March, Microsoft Patch

OTORIO, the leading provider of operational technology (OT) cyber and digital risk management solutions, today launched an open-source Microsoft Distributed Component Object Model (DCOM) Hardening Toolkit to protect OT systems against potential issues related to an upcoming Microsoft patch. The standalone open-source toolkit can be accessed by all organizations to detect and supply temporary workarounds for weak DCOM authentication applications.

OTORIO RAM2 users also automatically have access to a new alert in the Safe Active Query that allows detection across the entire network.

The OPC Data Access (OPC DA) protocol was launched in 1995 to enable the communication of real-time data between the programmable logic controller (PLC) and software within OT networks. However, OPC DA is based on DCOM technology, which includes security vulnerabilities. In 2008, Microsoft launched the non-DCOM-dependent OPC Unified Architecture (OPC UA) protocol, but many industrial businesses still use OPC DA.

In 2021, Microsoft acknowledged a critical vulnerability in its DCOM protocol and announced a hardening patch to strengthen the authentication between DCOM clients and servers. To minimize business disruption, it has released the patch in phases. The first patch introduced the ability

continue on page 19

to enable the hardening of the weak authentication levels in DCOM but was disabled by default; the second enforced the hardening by default with the option to disable it; the third rollout of the DCOM hardening patch automatically raised all non-anonymous activation requests from DCOM clients; and on March 14, 2023, Microsoft will issue a new patch that removes the option to enable unsecured DCOM altogether.

OTORIO's DCOM Hardening Toolkit enables users to quickly discover whether their networks include unsecured DCOM that will be rendered inoperable by the new patch. It then provides remediation instructions to make sure that organizations maintain full control of their OT devices.

"Organizations need to understand whether or not they have a problem, and that's where our toolkit comes in," said Yair Attar, CTO & Co. Founder of OTORIO. "If a company applies the March patch and loses critical visibility and communication between nodes in its network, it could experience significant financial losses. Our goal is to prevent that kind of catastrophe."

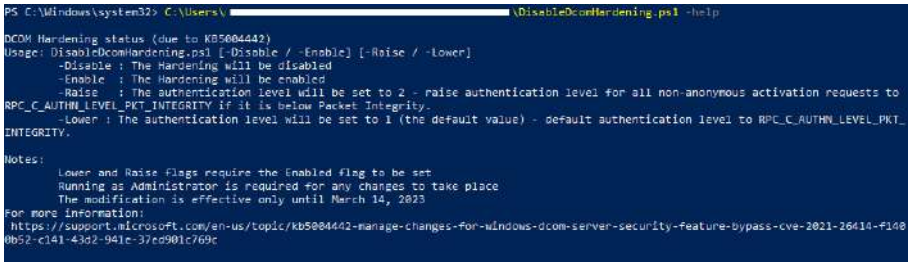
OTORIO's RAM2 collects and analyzes multiple data sources present in the OT environment, such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLC), distributed control systems (DCS), historian databases, engineering systems, and more. It then enriches this analysis with operational context, vulnerabilities, and exposures to assess security posture and identify and prioritize OT security threats.

Find the Hardening Toolkit on Github: https://github.com/otoriocyber/DCOM-HardeningTool

About OTORIO

OTORIO delivers proactive, orchestrated, and industrial-native OT cyber solutions. Effectively protecting industrial digitalization, OTORIO combines innovative technology, deep research, and proven real-world OT cybersecurity expertise.

For more information, please visit OTORIO.com. ■



SWEDISH TECHNOLOGY GROUP PURCHASES PATOL

Fire detection specialist Patol has welcomed the latest chapter in the company's development with the announcement that the business has been purchased by Sdiptech.

Patol has been manufacturing and supplying fire detection solutions across a wide range of industrial sectors since the business was formed in 1968. Under private ownership throughout this time, this announcement marks a significant investment from an international technology group based in Sweden that specialises in creating more sustainable, efficient, and safer societies.

The purchase is the twelfth business in the UK to be added to Sdiptech's portfolio and Patol joins the group's Special Infrastructure Solutions Business Unit. ■

SIEMENS APPOINTS NEW RSM

Siemens has expanded its sales team serving the UK and Ireland fire safety markets with the announcement of the appointment of Marios Malone.

Malone joins Siemens from the global power management company Eaton where he worked as a Regional Sales Manager in the Fire Division. At Siemens, he will be a Regional Sales Manager for the South, focusing on the company's Cerberus PRO open protocol fire protection system and its ASD (Aspirating Smoke Detection) range which uses red/blue optical technology to detect fire at the earliest incipient stage.

He brings more than 20 years of experience in the fire safety industry and is looking forward to the challenges his new role will bring. "Siemens has an excellent reputation in the fire safety arena, particularly in terms of its ongoing contribution to the digitalisation of systems. It is an interesting and exciting time to be involved as we move towards

Marios Malone, Regional Sales Manager, Fire Products, Siemens UK&I

increasingly intelligent systems which are now realising the potential afforded by cloud-based solutions."

Rob Yates, Siemens Head of Building Products Fire Safety in the UK and Ireland, comments – "We are delighted to welcome Marios to the team. His appointment reflects the increased interest in and adoption of Siemens solutions in the UK and Ireland, particularly Cerberus PRO, following the innovations brought about through the introduction of the IP8 version. I am sure Marios will make an important contribution in working with our network of partners to ensure we are offering effective protection for people and buildings based around a product portfolio focused on improving monitoring, maintenance, and planning.'

For further information on Siemens Fire Products, please visit www.siemens.co.uk/cerberus.

For further information on Siemens Smart Infrastructure, please visit www.siemens.com/smart-infrastructure. ■

SUSTAINABLE BATTERY POWER SOLUTION REACHES NEW SAFETY HEIGHTS IN ONE OF THE WORLD'S TALLEST WOODEN SKYSCRAPERS

- ABB delivers innovative and intelligent energy storage solutions for Sweden's landmark culture center
- Keeping visitors and staff safe with a unique battery energy storage solution for the wooden structure's sprinkler system
- In case of an energy failure, the ABB solution will provide sustainable backup power 24/7

The Sara Kulturhus is a state-of-the-art cultural venue and hotel in Skellefteå, Sweden. It is home to the city library, a museum and art gallery, and a theatre that stages 450 performances a year. Standing 75m tall, the 20-story timber building

continue on page 21

is one of the world's tallest wooden structures and is an international showcase for sustainable design and construction, with 100 percent of its electricity coming from renewable sources, including hydro and wind generation. The timber structure is so sophisticated that it removes more than twice the carbon emissions produced by the operational energy it uses and the embodied carbon from the production and transport of the materials used to construct it.

As a zero-emissions site, the Sara Kulturhus design required careful consideration and innovative solutions, such as its unique battery energy storage system (BESS), which was designed collaboratively by Skellefteå Kraft and ABB to provide reliable, clean power to the building's all-important fire sprinkler system.

In a timber construction like Sara Kulturhus , the sprinkler system is critical to keeping staff and visitors in the building safe. Traditionally, this fire protection system would be powered by emergency diesel generators, which serve as an onsite power supply should the mains power not be available. With Sara Kulturhus' commitment to sustainability, there is no diesel generator on site, so an alternative solution was required.

Skellefteå Kraft and ABB worked together on a bespoke energy storage solution to deliver maximum safety and reliability while harnessing the building's hydroelectric green electricity, received from the grid, which is used as the power supply. The bespoke BESS comprises six battery packs from local supplier Northvolt, AC and DC switchgear from ABB, inverters from EPC Power, and a transformer.

For Patrik Sundberg, Business Manager at Skellefteå Kraft, the BESS installation at the Sara Kulturhus was the culmination of a journey of collaboration between his company, ABB and Swedish battery supplier Northvolt. He said: "This is a truly sustainable, negative carbon building that operates on 100 percent renewable energy. Our solutions had to mirror this, so it was important to find a sustainable safety solution to power the sprinklers that didn't use diesel. To reduce the site's carbon footprint, it was also key to work with local suppliers, like battery manufacturer Northvolt. This innovative new concept really pushes the boundaries on the use of battery energy storage for fire prevention applications and will set a new standard for sustainable buildings in the future."

With the unique wooden design of the building, ABB's packaged solution was built and factory-tested off-site and then energized in the basement of Sara Kulturhus. To make it easier to manage the BESS and to ensure a reliable 24/7 power supply for the building's sprinkler system, the solution was supplied with a custom ABB eStorage OS energy management system to provide next-level energy monitoring, diagnostics, and data and analytics. As well as optimizing energy use internally, this advanced autonomous

AI technology interfaces with the building management system, allowing the center to interact with nearby buildings, so any excess renewable energy generated can be supplied to other parts of the city when required.

Sara Kulturhus CEO Anna Jirstrand Sandlund said: "This is a lighthouse project which embodies the region's values of delivering ecological, economical, and social impact to attract more people to Skellefteå and supports the green transition across North Sweden. With a wooden building of this scale, fire safety had to be one of our main considerations. By collaborating with ABB and Skellefteå Kraft, we have developed a unique solution that is now one of the highlights of our twice-daily guided tours for visitors. With the building itself now a blueprint for sustainability, we continue to work towards equaling its impact on the inside and inspiring our visitors and residents to become more sustainable."

Learn more about ABB's energy storage solutions offering by visiting solutions.abb/eStorage.

ABB (ABBN: SIX Swiss Ex) is a leading global technology company that energizes the transformation of society and industry to achieve a more productive, sustainable future. By connecting software to its electrification, robotics, automation, and motion portfolio, ABB pushes the boundaries of technology to drive performance to new levels. With a history of excellence stretching back more than 130 years, ABB's success is driven by about 105,000 talented employees in over 100 countries.

Electrifying the world in a safe, smart, and sustainable way, ABB Electrification is a global technology leader in electrical distribution and management from source to socket. As the world's demand for electricity grows, our 50,000+ employees across 100 countries collaborate with customers and partners to transform how people connect, live, and work. We develop innovative products, solutions, and digital technologies that enable energy efficiency and a low-carbon society across all sectors. By applying global scale with local expertise, we shape and support global trends, deliver excellence for customers and power a sustainable future for society.

For more information, please visit www.abb.com. ■

OPENTEXT ACQUIRES MICRO FOCUS

OpenText acquires Micro Focus for approximately USD $5.8 billion

OpenText™ (NASDAQ: OTEX), (TSX: OTEX) announced today that it has closed the previously announced acquisition (the "Acquisition" of Micro Focus International plc ("Micro Focus"), a leading provider of mission-critical software technology and services that help customers accelerate digital transformation. "I would like to welcome Micro Focus customers, partners, and employees to OpenText," said OpenText CEO & CTO Mark J. Barrenechea. "Digital life is life, and with Micro Focus' great products and talent, we will help organizations of all sizes accelerate their digital transformation." Barrenechea further added, "With this acquisition, OpenText's corporate mission expands to help enterprise professionals secure their operations, gain more insight into their information, and better manage an increasingly hybrid and complex digital fabric with a new generation of tools that include Cybersecurity, Digital Operations Management, Applications Modernization & Delivery, and AI & Analytics. This new generation of Information Management software will help organizations accelerate their digital transformation and drive growth while reducing costs."

Preliminary Financial Overview

Further information on our financial performance, as well as updated models, will be provided when OpenText reports its second quarter Fiscal 2023 financial & business results on February 2, 2023.

Closing Terms of the Acquisition

- Total purchase price of approximately USD $5.8 billion, inclusive of Micro Focus' cash and debt, subject to final adjustments
- Total purchase price is 2.3x Micro Focus' TTM revenues(1)
- Total purchase price is 6.7x Micro Focus' TTM adjusted EBITDA(2)
- Immediately accretive to F'23 adjusted EBITDA dollars
- Expected to be on the OpenText operating model within 6 full quarters or sooner
- Net leverage(3) expected to be less than 3x within 8 full quarters or sooner
- Consistent with previously announced cost synergies of $400 million, expect to balance the combined company through an approximate 8% workforce reduction due to the acquisition of Micro Focus
- "We have a structured and disciplined approach to M&A. The last six months of planning has led us to a defined integration plan to deliver on our committed outcomes. We are ready and excited about winning the Information Management market, strong customer outcomes, and company growth and expanded cash flows," concluded Barrenechea.

About OpenText

OpenText, The Information Company™, enables organizations to gain insight through market-leading information management solutions powered by OpenText Cloud Editions.

For more information about OpenText (NASDAQ: OTEX, TSX: OTEX), please visit opentext.com. ■

GALLAGHER PREDICTS - "CHAMPIONING THE CUSTOMER IN 2023 WILL DRIVE ACCESS CONTROL INNOVATIONS"

Global security manufacturer Gallagher is predicting the global market will remain difficult for businesses throughout 2023 but believes that its customer-centric strategy will help the company to innovate its way to delivering outstanding value to customers, despite a challenging economy.

Speaking about Gallagher's strategy, Chief Architect of Gallagher Security, Andrew Scothern said: "As a company, we strongly believe that championing the customer will drive access control innovations. Our long-term plan is to deliver a fully cloud-based enterprise solution, and we feel it's important to work closely with customers as they make the transition to an enhanced security software ecosystem. We believe security technology players need to take the customer on the journey of product development in order to truly meet their complex access control needs. Therefore, at Gallagher Security, we'll be focused on upgrading and maintaining systems using a hybrid approach of both on-premise and cloud-based systems".

Key to Gallagher's customer-centric approach is recognizing that customers want choice, which means

continue on page 23

ensuring the company never takes away the option for customers to be able to host their access control software themselves. In addition, Gallagher aims to provide compelling value through a series of flexible, scalable cloud-based services – for those that are comfortable taking that step. "Along with choice, customers also want ease of deployment with a rich set of integration points," Andrew explains.

"The commitment to building rich Application Programming Interfaces (APIs) and integration points ensures that customers can extend the site management software ecosystem in ways that suit the way they work, and ensures Gallagher builds a comprehensive collection of partners to meet the complex needs that customers have." This approach requires more work and a longer development time for Gallagher; however, the payoff is being able to offer a solution that is truly customized to customers' business needs and the ability to react quickly to adjust the Gallagher product based on their feedback.

Source of Truth

Thanks to its close working relationship with customers, Gallagher has been able to recognize the developing trend of access control products being used as a source of truth for information in customers' wider processes and ecosystems.

"With more focus on health and safety and knowing how building spaces are being utilized, the importance of having first-class integrations to get information in and out of the access control system is becoming increasingly important," said Andrew.

"This is another reason why our ongoing investment into our integration capabilities is so crucial to being able to evolve with our customers, design for limitless scale for growing organizations, and regularly deliver value."

For further information on Gallagher's world-class security solutions, please visit https://security.gallagher.com/ ■

TDSI HONOURED BY THE BSIA FOR 30 YEARS OF MEMBERSHIP

Integrated security manufacturer reflects upon three decades of working with the British Security Industry Association to promote British security products and services in the UK and worldwide

Integrated security manufacturer TDSi has been honoured by the BSIA (British Security Industry Association) in recognition of its 30 years of membership. To mark the occasion, TDSi Managing Director John Davies was presented with an Anniversary Trophy by BSIA Director John MacAskill MSyl at the Intersec 2023 event in Dubai in January.

John Davies commented, "It's an honour to have been associated with the BSIA for the last 30 years and to have been able to contribute to its fantastic work across the whole British Security Industry throughout that time. The industry has evolved and grown beyond all recognition over the last three decades, as has TDSi, but the BSIA continues to be a positive unifying element which promotes excellence, good business practices and trust, which define British security worldwide and uphold its well-deserved reputation. Here's to the next 30 years!"

Following the presentation of the Anniversary Trophy, a spokesperson for the BSIA also commented, "During this time, TDSi have been able to help shape the direction of the security industry, by sharing their industry insights

through playing an active role in our Access and Asset Protection and Export Council sections, with John also being current AAP Section chair. We look forward to our continued relationship working with and representing you as Your Association."

For more information on TDSi and its products, please visit www.tdsi.co.uk ■

TEXECOM LAUNCHES THE MIDNIGHT BLACK COLLECTION

Texecom has announced the availability of its Midnight Black Collection.

Working in harmony with darker environments, The Midnight Black Collection has been created for businesses and sites that require or prefer a security solution that offers unrivalled, contemporary, and discreet protection that compliments their surroundings.

Texecom's Midnight Black Collection includes the complete range of Capture Grade 2 motion detectors, Premier Elite LCDLP / LDLCP-W keypads, Impaq S / SC/ SC-W, and Micro Contact-W / Micro Shock-W perimeter detectors.

Discover the complete Midnight Black Collection now:

- **Capture –** Our highest performing, most reliable, easiest to install range of detectors ever.
- **Wired and Wireless Keypads –** With intuitive operation, ergonomic design, and backlit keys, the large blue LCD menu system is simple to use and can include proximity tags for additional ease in arming and disarming.
- **Impaq S Series –** Perimeter protection taken to the next level. The Impaq S Series provides a step change in shock detection performance, with VIBER™ Accelerometer Technology for class-leading and standards-exceeding intruder detection.
- **The Micro Contact-W –** Provides unobtrusive, discreet security.
- **The Micro Shock-W –** Designed to detect and analyse a forcible shock and provide early warning of an attempted intrusion before a break-in occurs, ensuring the safety of people and property inside.

For more information, please visit www.texe.com. ■

VIKING ANALYTICS RAISES SERIES A OF MORE THAN € 3MN FOR GLOBAL EXPANSION

Integrated security manufacturer reflects upon three decades of working with the British Security Industry Association to promote British security products and services in the UK and worldwide

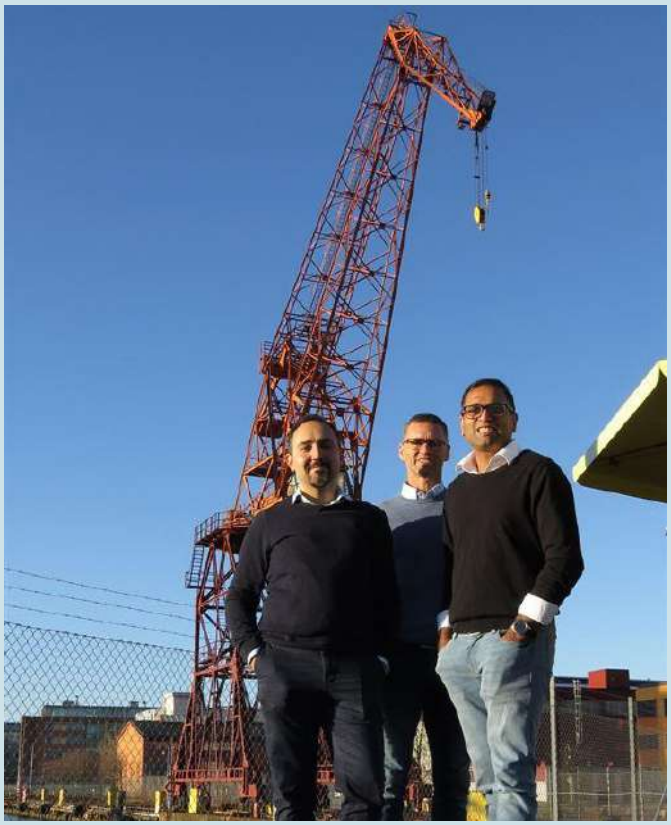
- Sweden-based Viking Analytics closed its Series A funding round with the support of Finindus, Industrifonden, and ABB
- This round will allow Viking Analytics to accelerate the development of machine health monitoring solutions.
- Viking Analytics has also secured a commercial agreement with ABB to bring its machine health monitoring solution to ABB's switchgear products.

Viking Analytics AB, the Swedish company developing AI-based machine health monitoring technology, today announced the closing of its Series A round. Viking Analytics' Series A round was co-led by Belgium-based Finindus (backed by ArcelorMittal) and Sweden-based Industrifonden, with ABB and existing investors also participating in the round.

The company also disclosed it had secured a commercial agreement with ABB for monitoring their customers' switchgear products. The investment funds in mobility and smart industrial technologies and the commercial contract serve as recognition of the company's capabilities and will allow Viking Analytics to accelerate its technological development and scale the commercialization of its solutions.

Dr. Rajet Krishnan, co-founder, and CEO of Viking Analytics, comments, "We are excited to have closed an oversubscribed round in an unusually tough environment. This investment is a strong testament to our unique value proposition, market position, and technology readiness. We believe that our new investors will bring tremendous value with deep industry expertise and networks to our journey in enabling in remote machine health monitoring."
Let's Connect

Starting operations in 2018, Viking Analytics is on a mission to enable every industrial service company (like maintenance companies, OEMs, and system integrators) to monitor more machines reliably. Vikings' proprietary solution prioritizes the machines that need attention while providing relevant explanations for the prioritization. Furthermore, experts can provide feedback based on the priority list and recommend actions. With the Viking solution, service companies can offer reliable remote monitoring services with less false alarms and without in-house AI teams. Vikings' unique approach of augmenting human experts to becoming "super-experts" is steadily gaining market acceptance, as proven by more than 20 customers globally.



"Viking Analytics convinced us of their approach to machine health monitoring," says Roel Callebaut, Investment Manager at Finindus. "Through numerous conversations with industry experts, we understood they are solving the issues that prevented previous predictive maintenance solutions to be used for non-critical assets."

Karolina Bjurehed, Investment Director at Industrifonden, states. "We're impressed by what the team has accomplished so far and are happy to support this technological development and innovation in the industry. Not only does it enable more efficient control of the product line, but it's also more sustainable.
Chao Wu, Principal at ABB Technology Ventures, expresses, "With the pressure on to ensure uptime and prolong the lifecycle of electrical assets, the partnership allows us to develop analytics that will help customers maintain their operations and cut costs. Customers will get the insights they need to make informed decisions about their electrical equipment fleet and take preventative actions to avoid costly failure. We look forward to continuing our close collaboration with Viking Analytics to further develop and scale new AI software solutions in the future." ■

Digital Transformation in Physical Security Industry

Images by Freepik

Digital transformation in the physical security industry refers to the integration of digital technologies, like artificial intelligence, the internet of things (IoT), and cloud computing into traditional security systems and processes. Moreover, this transformation aims to improve the efficiency, accuracy, and overall effectiveness of physical security measures. By incorporating digital tools, physical security organisations can monitor, analyse and respond to security threats in real-time, as well as automate routine tasks, freeing up personnel to focus on more strategic and essential responsibilities. The goal of digital transformation in the physical security industry is to enhance security and safety while also reducing costs and improving customer experience.

Importance of Digital Transformation in Physical Security

Digital transformation in physical security is crucial for several reasons, and it becomes important for us to understand it in detail. Here are a few reasons to check out:

- **Improved Efficiency:** Digital technologies automate routine tasks and improve workflows, making security processes quite efficient and reducing the workload on personnel.
- **Enhanced Security:** Integrating advanced technologies, such as AI and IoT, provides a more comprehensive and proactive approach to security. This leads to faster response times, improved threat detection, and heightened security.
- **Real-time Monitoring:** Digital tools allow for real-time monitoring of security systems, providing faster response times to incidents and quick resolution of security threats.
- **Data Analytics:** Digital transformation provides access to vast amounts of data that can be analysed to identify trends as well as patterns that are used to make better decisions about security measures.
- **Cost Savings:** Automating routine tasks and reducing manual labour through digital technologies can result in significant savings for physical security organisations.
- **Improved Customer Experience:** By providing a more efficient, proactive, and secure physical security experience, customers can feel confident and safe, leading to an improved overall experience.

Overall, digital transformation in physical security is essential in today's fast-paced and constantly changing technological landscape. By incorporating digital technologies, physical security organisations can remain competitive and provide special security measures that meet the evolving needs of their customers.

Key Elements of Digital Transformation

According to Microsoft's Case Study in reference to the Future of Physical Security, a successful digital transformation requires three elements: digital thought leadership, unified strategy, and persistent innovation.

- **Digital Thought Leadership:** Strong digital thought leadership is critical to driving digital transformation. This means having leaders who understand the potential of digital technology and are willing to take bold steps to adopt and integrate these technologies into the organisation. Furthermore, you can achieve digital thought leadership by changing the mindset, putting the customer first, building deep cross-

and building a digital culture all around.

- **Unified Strategy:** A unified strategy that is aligned with the organisation's goals and objectives is essential for a successful digital transformation. This includes a clear understanding of digital maturity, a roadmap for digital transformation, and a plan for implementing new technologies and processes.
- **Persistent Innovation:** Digital transformation is an ongoing process, not a one-time event. Organisations must be persistent in their efforts to innovate and adopt new technologies to stay ahead of the curve. This requires a culture of innovation, a willingness to experiment and learn, and an ongoing investment in new technologies and processes. While partnering with Accenture, Microsoft's report highlights, "the future of physical security with digital transformation will be drastically different than physical security today. Teams will be able to predict and mitigate threats before they occur, freeing up resources to focus on strategic action and decisions. Every step forward in transformation is a step closer to realising this vision."

In conclusion, a successful digital transformation requires strong digital

Images by Freepik

Digital transformation is an ongoing process, not a one-time event. Organisations must be persistent in their efforts to innovate and adopt new technologies to stay ahead of the curve.

thought leadership, a unified strategy, and persistent innovation. By focusing on these elements, businesses can transform themselves and gain a competitive advantage in an increasingly digital world.

Impact of Digital Transformation on Physical Security

The impact of digital transformation on physical security can be significant and far-reaching. Since the physical security industry has taken an active approach lately, according to research, the addressable market estimate is likely to grow to $232.5 billion by 2027. Here are some of the critical impacts:

- **Increased Automation:** Automating routine tasks and processes through digital technologies can improve efficiency and reduce the workload on personnel, freeing them up to focus on more strategic responsibilities.
- **Improved Threat Detection:** Advanced technologies, such as artificial intelligence and machine learning, can improve threat detection and response times, providing a more proactive and comprehensive approach to security.
- **Enhanced Data Management:** Digital transformation provides access to vast amounts of data to identify trends and patterns, providing organisations with valuable insights to make better decisions about security measures.
- **New Business Models:** The transformation process can also open up new revenue streams for physical security organisations. For instance, organisations can monetize data they collect, analyse, or offer new services based on the latest digital technologies.

In short, the digital transformation in physical security is transforming the industry and leading to significant improvements in security, efficiency, and customer experience. With the rapid pace of technological transformation, it is important for physical security organisations to adopt and integrate digital technologies to remain competitive and provide the best possible security measures.

Key Benefits

Here are the key benefits of digital transformation:

- Improved Threat Detection
- Increased Efficiency
- Enhanced Data Management
- Efficiency in Decision Making
- Improved Customer Experience

Images by Freepik

Challenges of Implementing Digital Transformation in Physical Security

While digital transformation in physical security can bring many benefits, there are also challenges that organisations must overcome to implement it successfully. Some of the key challenges include:

- **Lack of Technical Expertise:** Implementing advanced digital technologies can require a high level of technical expertise, which may not be readily available within physical security organisations.
- **Integration with Legacy Systems:** Integrating new digital technologies with existing legacy systems can be challenging and require significant investment when it comes to time and resources.
- **Resistance to Change:** Some personnel within physical security firm may be resistant to change and may not be comfortable with new digital technologies.
- **Data Privacy and Security Concerns:** With the integration of digital technologies, there are concerns about the privacy and security of sensitive data. Further, organisations must ensure appropriate security measures are in place to protect sensitive information.
- **Budgetary Constraints:** Implementing digital transformation can require significant investment, and businesses may need to secure funding and allocate budgets to support these efforts.
- **Technical Complexity:** Digital technologies can be complex and require significant resources and expertise to implement and maintain.

Despite these challenges, digital transformation in physical security is essential for organisations to remain competitive and provide the best possible security measures. To overcome these challenges, organisations must take a strategic and collaborative approach involving all stakeholders, including personnel, customers, and partners, to ensure a successful implementation.

The Best Practices for Implementing Digital Transformation

There are a few practices that can be employed to implement a full digital transformation by focusing on the primary areas of transformation. Let's have a look!

- **A Clear Strategy:** Businesses should develop a clear strategy for digital transformation. This can be done by outlining the objectives, goals, and expected

By following these best practices, organisations can successfully implement digital transformation in physical security and reap the benefits of improved efficiency, enhanced security, and an improved customer experience.

outcomes. This will also ensure that all efforts are aligned and focused on achieving the desired outcomes.

- **Involve Stakeholders:** Involve all stakeholders, including personnel, customers, and partners, in the digital transformation process to ensure their needs are taken into account and to gain buy-in and support.
- **Invest in the Right Technologies:** Businesses should invest in the right technologies that are fit for purpose and align with their objectives. This can include advanced technologies such as artificial intelligence and the internet of things (IoT).
- **Foster a Culture of Innovation:** Organisations should foster innovation and encourage personnel to experiment with new technologies and approaches. Furthermore, it will help to drive continuous improvement and innovation.
- **Focus on Data Management:** Data management is critical for digital transformation, and organisations should focus on collecting, analysing, and utilising data to make informed decisions about security measures.
- **Continuously Evaluate and Improve:** Digital transformation is an ongoing process, and businesses that are on a transformation journey should continuously evaluate and improve their systems and processes to ensure they remain relevant and practical.

By following these best practices, organisations can successfully implement digital transformation in physical security and reap the benefits of improved efficiency, enhanced security, and an improved customer experience.

Wrapping Up

Moreover, digital transformation in the physical security industry is crucial in enhancing the security of assets and properties. Furthermore, integrating digital technology into traditional physical security systems provides organisations with more efficient, effective, and secure ways to protect their assets. By embracing digital transformation, organisations can stay ahead of the curve while gaining a competitive advantage and securing their assets in an increasingly digital world. ■

Images by Freepik

COMING SOON

MAR 29 – 31 2023
ISC West 2023
Las Vegas, USA
https://www.discoverisc.com/global/en-us/isc-west.html

APR 25 – 27 2023
The Security Event 2023
Birmingham, United Kingdom
https://www.thesecurityevent.co.uk

APR 27 – 29 2023
Secutech India 2023
Mumbai, India
https://secutechindia.in.messefrankfurt.com

APR 26 – 28 2023
Secutech Taiwan 2023
Taipei, Taiwan
https://secutech.tw.messefrankfurt.com

AUG 16 – 18 2023
Secutech Vietnam 2023
HCMC, Vietnam
https://secutechvietnam.tw.messefrankfurt.com

SEP 11 – 13 2023
GSX 2023
Dallas, USA
https://www.gsx.org

OCT 3 – 5 2023
Intersec Saudi Arabia 2023
Riyadh, Saudi Arabia
https://www.intersec-ksa.com

NOV 1 – 3 2023
Secutech Thailand 2023
Bangkok, Thailand
https://secutechthailand. tw.messefrankfurt.com

Security Solutions Today is available on issuu!

issuu.com/securitysolutionstoday

Or download our e-magazine at

sst.tradelinkmedia.biz

SUBSCRIPTION FORM

Email your order to:
yvonne.ooi@tradelinkmedia.com.sg

PRINT

Please (√) tick in the boxes.

Southeast Asia Building
Since 1974

Southeast Asia Construction
Since 1994

***1 year** (6 issues) per magazine*

Singapore	SGD$70.00
Malaysia / Brunei	SGD$120.00
Asia	SGD$180.00
America, Europe	SGD$220.00
Japan, Australia, New Zealand	SGD$220.00
Middle East	SGD$220.00

Bathroom + Kitchen Today
Since 2001

***1 year** (4 issues) per magazine*

Singapore	SGD$40.00
Malaysia / Brunei	SGD$90.00
Asia	SGD$110.00
America, Europe	SGD$160.00
Japan, Australia, New Zealand	SGD$160.00
Middle East	SGD$160.00

DIGITAL

Lighting Today
is available on digital platform.
To download free PDF copy,
please visit:

http://lt.tradelinkmedia.biz

Lighting Today
Since 2002

Security Solutions Today
is available on digital platform.
To download free PDF copy,
please visit:

http://sst.tradelinkmedia.biz

Security Solutions Today
Since 1992

Personal Particulars

Name:

Position:

Company:

Address:

Tel: **E-Mail:**

IMPORTANT

Please commence my subscription in
(month/year)

Professionals (choose one):

Architect	Landscape Architect	Interior Designer	Developer/Owner
Property Manager	Manufacturer/Supplier	Engineer	Others

Bank transfer payable to:
Trade Link Media Pte Ltd
Bank Details

Account Name:	Trade Link Media Pte Ltd
Account Number:	033-016888-8
Name of Beneficiary Bank:	DBS Bank
Address of Beneficiary Bank:	12 Marina Boulevard, DBS Asia Central, Marina Bay Financial Centre Tower 3, Singapore 018982
Country:	Singapore
SWIFT Address/Code:	DBSSSGSG

PAYNOW to:
Trade Link Media Pte Ltd

PAYNOW option is applicable for **Singapore companies only**.

Company Registration Number: 199204277K

* GST inclusive (GST Reg. No: M2-0108708-2)

ADVERTISE WITH US TODAY!

Email us at info@tradelinkmedia.com.sg.

Scan to visit our website