NATIXIS
INVESTMENT MANAGERS

THEMATICS
asset management

INSIGHTS

When OT meets IT: Bridging the cybersecurity gap for critical infrastructure

Frédéric Dupraz,
Senior Portfolio Manager
Thematics Asset Management

Karen Kharmandarian,
Chief Investment Officer
Thematics Asset Management

Matthieu Rolin,
Portfolio Manager
Thematics Asset Management

Alexandre Zilliox,
Portfolio Manager
Thematics Asset Management

KEY TAKEAWAYS

All crises tend to expose vulnerabilities and accelerate transformation. The uniqueness from which the Covid-19 crisis has stemmed has shone a new light on the potential disruption to operational and technological infrastructure, as an increasingly connected world has had to operate remotely.

Our increasingly connected world means that it has become possible for unwanted actors to infiltrate and compromise nuclear power stations, electricity grids and traffic lights – maybe even democratic elections and referenda.

Many organisations have increasingly moved away from isolated, manually controlled **operational technology (OT)** systems to an environment in which physical processes are controlled with sophisticated and interconnected information technology (IT) equipment.

Integrating OT with IT will have a great impact on network structure and will force companies to think of a more effective way to protect their network. With the addition of new connected devices, the surface of attack will increase tremendously – and any new device connected will be an entry point for an attacker.

Of course, once the cybersecurity gap is closed for critical infrastructure, the nature of the industry means that there will already be another surfacing somewhere else in cyberspace. This makes cybersecurity – like the safety of governments, individuals and corporations more generally – a perennial theme in our lives and in our investments.

The primary forces driving the need for operational and information technology security

All crises tend to expose vulnerabilities and accelerate transformation. The uniqueness from which the Covid-19 crisis has stemmed has shone a new light on the potential disruption to operational and technological infrastructure, as an increasingly connected world has had to operate remotely.

New threats and opportunities have emerged that go beyond what even the most enlightened corporations, governments and individuals could have envisaged. The root causes of disruption have been laid bare as technology, globalization, evolving demographics and resource scarcity all continue to shape societies and economies across the globe. With insecurity becoming the new normal, nations are becoming increasingly sensitive to protecting populations and their wealth as cyber risk emerges as a major threat.

The large-scale sabotage of computerized networks, systems and activities, commonly referred to as 'cybergeddon', conjures up notions of fear, loss of control and inevitability. But while the threats are real, so too are the opportunities.

Reflecting on how corporations and governments have adapted to the current situation through technology advancements and societal progress, opportunities are presenting themselves that can lead to a digitally-driven industrial revolution. Catalysts such as 5G embody a quantum leap in capability for the connected economy, unlocking the potential of the **Internet of Things (IoT)** by connecting everything from manufacturing machinery to domestic appliances with unprecedented speed and capacity.

As of 2019, more than 26 billion IoT devices were active; by 2025, it is estimated that there will be 152,200 IoT devices connecting to the internet per minute. Of course, with that comes an increased number of threats and risks of networks being compromised. Yet the combination of artificial intelligence and robotics could also empower manufacturers.

> "Nothing is particularly hard if you divide it into small jobs.
>
> **Henry Ford,** founder of the Ford Motor Company

Connected worlds

Since the time of Henry Ford, the narrative for manufacturing has been finding ever greater efficiencies in manufacturing processes. Today, 5G allows a manufacturer to create 'connected factories', with sensors recording data on everything from temperature and vibrations to the quantities of material used. This can in turn generate tremendous efficiency gains: the reduction in maintenance costs through predictive maintenance, a reduction of total machine downtime through remote monitoring and control, or even productivity increases through real time energy consumption.

It is important, however, to explore the other side of the digital coin. Digital's disruptive power can open doors and provide attackers with the ability to disrupt value chains and turn data and information theft into a highly effective weapon. Cyber attacks can often go undetected for months and, once networks have been penetrated, it can then be highly challenging to secure systems.

Attacks expose corporations and, increasingly, governments and national agencies to massive threats, which reinforces the need for cutting edge cyber security solutions. In light of how the world has adapted as businesses and individuals shift online, IT architectures are in the process of being rethought from the ground up.

As such, we have observed the necessity for economic agents to bridge the gaping cybersecurity gap to safeguard critical infrastructure and ensure the proper functioning of markets and economies.

Operational technology (OT)

Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events.

Internet of Things (IoT)

The internet of things describes the network of physical objects—a.k.a. 'things'—that are embedded with sensors, software, and other technologies and connect to or exchange data with other devices and systems over the Internet.

The shifting frontier of cybersecurity

Our increasingly connected world means that it has become possible for unwanted actors to infiltrate and compromise nuclear power stations, electricity grids and traffic lights – maybe even democratic elections and referenda. And as we increase those connections there's simply more potential for everything to be hacked.

The scale of the challenge for the cyber security industry is considerable. Just consider what happened in 2013. On a normal April afternoon, the entire internet – all 3.7 billion connected computers and devices in factories, pockets and offices around the world – was pinged by a single operator.

That ping revealed about 114,000 manufacturing control systems vulnerable for attack, about 13,000 of which could be accessed without inputting a single password. If nothing else, this event acted as a wakeup call for the cybersecurity industry.

Logic bombs and weaponized worms

Perhaps one of the earliest examples of a devastating industrial hack occurred in 1982. The CIA successfully planted a so-called 'logic-bomb' into the **Supervisory Control and Data Acquisition (SCADA)** system controlling the USSR's Siberian natural gas pipeline. The result was what the Washington Post called "the most monumental non-nuclear explosion and fire ever seen from space[1]."

A SCADA system is a computer application used to monitor and control a plant or equipment at the supervisory level. They are used in many different industries to collect and analyse real-time data, as well as to control functions. This makes them a target to malicious hackers. And because of that it's important to defend your system against SCADA threats and attacks.

In 2010, Stuxnet provided a wake-up call to SCADA systems around the world. One of the most complex **malwares** to date, it was considered the first known threat to target specifically SCADA systems in order to control networks.

An allegedly state-sponsored weapon, the Stuxnet worm targeted the **PLC systems** in Iran's nuclear program, causing centrifuges to spin out of control without triggering alarms. Before it was caught, the attack was able to destroy up to one fifth of the country's nuclear centrifuges and set its nuclear program back a decade.

A lesson learned from Stuxnet is that a sophisticated threat can likely attack any system, so the ability to detect and recover from a cyber-attack is critical. Sure enough, in May 2012, Russia's Kaspersky Lab – one of the world's biggest producers of anti-virus software – discovered another highly sophisticated virus directed at Iran.

Unlike Stuxnet, the Flame virus – which ran undetected for years – was designed to steal PDF files and **AutoCAD** drawings. It meant the originator of the attack was after designs, plans and preciously guarded IP data locked inside some of the country's biggest industrial facilities[2].

Hacking dams and disrupting grids

In 2013, a small dam in New York was accessed by Iranian hackers. This intrusion was not elaborate, since it was simply a test by the attackers to see what they could access. The small utility, called Bowman Dam, controls storm surges. Its SCADA system was connected to the Internet via a cellular modem. The SCADA system was at maintenance during the time of the attack, so no control features were available; only status monitoring.

It's assumed that the dam was attacked due to its vulnerable Internet connection and lack of security controls, rather than a targeted cyber-attack. And while we don't know who was conducting the intrusion, we do know the technical sophistication they showed by directly manipulating SCADA equipment. It's just another reminder that when SCADA systems are directly exposed to the internet, they become an easy target for any potential hacker[3].

Two years after the Bowman Dam hacking, the first known successful cyber-attack on a power grid cut

PLC systems
Industrial digital computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, robotic devices, or any activity that requires high reliability, ease of programming, and process fault diagnosis.

AutoCAD drawing
Detailed 2D or 3D illustration displaying the components of an engineering or architectural project.

Supervisory Control and Data Acquisition (SCADA)
Control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLC) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery.

Malware
Umbrella term used to refer to a variety of hostile or intrusive software: computer virus, worms, Trojan horse, ransomware, spyware, adware, scareware, etc

electricity to nearly a quarter of a million Ukrainians. The attackers shut off power at 30 substations, leaving around 230,000 people without electricity for up to six hours.

They used **spear phishing emails,** a low-tech approach to launch such an attack – a trend that's still relevant today, with phishing being used against critical infrastructure. Awareness to these risks is therefore a major factor in the success of these simplistic approaches.

Precisely a year after that attack, another hit the country – this time targeting the Pivichna substation near Kiev, causing an hour-long blackout in the surrounding area. The significance of this attack was that it led people to question whether these attacks were practice for something still more powerful.

Indeed, Eugene Kaspersky, cybersecurity expert and CEO of Kaspersky Labs, issued a warning to the world that we could be on the brink of turmoil, with hackers closing in on the features of critical infrastructure[4].

Penetrating pacemakers and exposing prisons

Infrastructure hacking can even extend to medical implants, which are seen by some as the new frontier. In 2019, US regulators and security experts sent out an official warning that hackers could now access critical medical equipment – including pacemakers and insulin pumps – with potentially deadly results[5].

And in early 2020, hackers secretly broke into the systems of a US IT firm, SolarWinds, which had 33,000 customers – including Fortune 500 companies such as Microsoft, Cisco, Intel and Deloitte, as well as US government agencies, including the Treasury Department. The cyber-attack went undetected for months and multiple networks were penetrated with no quick fix.

Indeed, the US government confirmed that it could be years before the networks were secure again. And because it exposed not only leading corporations but also government agencies to attacks, it remains one of the largest breaches in recent memory.

Another recent example involved a group of hackers that broke into the security-camera data collected by Silicon Valley companies, which gained them access to live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, prisons and schools. Companies that had footage exposed included the carmaker Tesla.

Some of the cameras used facial-recognition technology to identify and categorize people captured on the footage. One of the videos even shows officers in a police station in Stoughton, Wisconsin, questioning a man in handcuffs. Have you ever imagined your identity being exposed like this? If so, would you still buy security cameras from that company?

Furthermore, increasing global regulatory oversight is also making governments, corporations and individuals more aware of safety around data privacy and protection. This is leading to significant investments in cybersecurity solutions.

When IT security collides with operational security

So why has this all been happening? And how will it manifest in the future?

In short, as technology continues to evolve, many organisations have increasingly moved away from isolated, manually controlled operational technology (OT) systems to an environment in which physical processes are controlled with sophisticated and interconnected information technology (IT) equipment.

As more devices become 'smart' through wireless connectivity, OT systems that once required hands-on manipulation – such as adjusting a valve or flipping a switch – can now be controlled remotely. Many of these OT systems are becoming part of an organisation's critical infrastructure.

Take NASA. Its OT systems are used to test rocket propulsion systems, control and communicate with spacecraft, and operate ground support facilities. They

Spear phishing emails

Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

are also associated with the electrical power, heating and cooling systems, and other supporting infrastructure.

While the convergence of IT and OT can lead to cost savings and other efficiencies, it also means OT systems are potentially vulnerable to the types of security challenges more common to IT systems, including malicious hacking[6].

The cyberphysical challenge and the need for ageing infrastructure to adapt to an increasingly connected surface

Integrating OT with IT will have a great impact on network structure and will force companies to think of a more effective way to protect their network. With the addition of new connected devices, the surface of attack will increase tremendously – and any new device connected will be an entry point for an attacker. The old 'castle and moat' architecture is outdated and doomed.

The 'castle and moat' model explained

Let's imagine a castle that is surrounded by a deep moat. There's only one way in and out of the castle: over a drawbridge that is heavily guarded. Anyone attempting to enter the castle must pass a rigorous security check by the guards. Once that person is trusted, they're allowed free access to the castle and everything in it. In fact, everyone inside the castle is trusted by default.

This is where the problem lies: if someone manages to bypass the guards and enter the castle without permission, they will never be checked again – and they will be able to come and go in the castle without hindrance. Now, imagine if we multiply the number of entrance doors: this will multiply the risk of intruders walking around the castle with impunity.

That's why network security needs a new model: the 'zero-trust' approach.

The 'zero trust' approach explained

The **'zero trust'** approach is radically different from the castle and moat model. Zero trust security means that no one is trusted by default either inside or outside a corporate network, so verification is required from everyone who wants access to resources on the network.

It requires strict identity verification for every person and device attempting to access resources on a private network, whether they're inside or outside the corporate network perimeter. The emphasis is on identity, which means one can multiply the entry points to the network without any problem, since each time one has to show proof of identity.

The disruptive catalysts forcing the convergence of OT with IT

AI and automation's impact on industry

When we talk about AI and automation in cybersecurity it refers, in most cases, to **Machine Learning (ML).** This is a subset of AI where the aim is to teach a machine how to make a decision on its own or answer a question without necessarily giving the machine very specific instructions or without programming it in order to cover all possibilities.

How are AI & ML transforming the industry?

To put it simply, humans and traditional cybersecurity solutions are not sufficient today:

- Traditional solutions are monitoring, scanning and looking at known threats and risks while ML-based solutions can help detect new anomalies (malwares, viruses, and so on), prevent the attack and orchestrate a response if needed. If we take the example of **MFA (multi-factor authentication)**, ML tools could detect if a specific user is connecting on a network from an unusual device or location and act by blocking the access or asking for another authentication factor (one-time password, facial

Zero trust
An approach to the design and implementation of IT systems. The main concept behind zero trust is that devices should not be trusted by default, even if they are connected to a managed corporate network and were previously verified.

Machine Learning (ML)
The study of computer algorithms that improve automatically through experience and by the use of data.

Multi Facto Authentication (MFA)
An electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism.

recognition, fingerprint scan, and so on). Traditional solutions usually don't take into account the historical behaviour of a user, a device or a network, leaving more chance for an attack to succeed.

- The number of devices that need protection is now massive: whether it's computers, smartphones, servers, industrial machines or cars, everything is connected, which increases the surface of attacks. Humans just can't analyse all the threats and abnormal behaviour that takes place in enterprises. This is where automation and AI step in. For example, CrowdStrike, a leading vendor of endpoint security solutions with close to 10,000 customers, captures more than 5 trillion events per week on its platform.

5G: greater connectivity and interfaced systems comes with increased critical infrastructure exposure

The 5G standard, relative to 4G, offers two key features:

1. the ability to connect more than a thousand times as many objects on the network,
2. latency reduced to 1 millisecond.

It is these two characteristics that will be used to connect the productive apparatus. Indeed, low latency is an essential element for taking control of a machine or a robot – the commands given must be received instantly by the connected device. Meanwhile, the ability to connect a very large number of objects is also key to being able to control a large fleet of objects.

Companies will also be able to create private 5G networks – which are faster and better suited than Wi-Fi networks – to connect operating technologies. The main questions remain around the adoption rate of 5G and the implementation of the technology.

The implications of re-onshoring

As we have witnessed during the Covid-19 pandemic, overreliance on distant geographies for manufacturing poses both economic and national security risks. Governments around the world have taken good note of it and we are seeing incentives for re-onshoring some of these manufacturing capacities closer to demand.

The latest and perhaps most striking example is taking place in the semiconductors industry, which is facing perhaps the biggest shortage episode in its history. This is affecting several end-markets, including consumer electronics, automotive and industrials.

This re-onshoring trend can be witnessed mostly in developed economies that have, in most cases, underinvested in their industrial footprints and/or relocated their plants to low-labour cost countries for decades. It is therefore fair to assume that enterprises and governments will try to build modern manufacturing capacities, which should drive improved demand for connected machines, devices and software platforms that will handle the data generated at the manufacturing level.

In a nutshell, this should act as a catalyst for **Industry 4.0 and the industrial IoT (IIoT)**: McKinsey estimates that the IIoT market will grow by 12% per year until 2025, reaching a market size of $500 billion[7] – all sustained by the deployment of 5G. The second derivative of this will be the need to secure the above tools, and the data flowing from them, which creates a new area of growth for cybersecurity.

The disruptive catalysts forcing the convergence of OT with IT

If we were to go back a decade or so ago, any conversation about protecting companies from would-be hackers would largely be about protecting the servers or IT equipment in the broadest sense: protection of physical equipment. It's the move from physical storage to virtual storage, or cloud computing, and the increasing connectivity of operational technology that has completely changed the way companies need to think about cybersecurity.

What's more, one result of the pandemic has been the increased attention given to remote worker security. Many employees have been using their personal devices for two-factor authentication, as well

Industrial Internet of Things (IIoT)

Refers to interconnected sensors, instruments, and other devices networked together with computers' industrial applications, including manufacturing and energy management.

as using mobile app versions of Instant Messaging and Video Conferencing clients – such as Teams and Zoom. The lines have therefore become blurred between personal and professional life, which only increases the risk that sensitive information will fall into an insecure environment.

According to a report by networking giant Cisco, 52% of its surveyed respondents said that mobile devices are a major challenge when it comes to cyber security[8]. Clearly, firms are not only forced to protect their systems and the workplace in the physical sense, but they are now forced to protect them in a virtual sense – and all the while ensure that any remote connections to virtual systems and workplaces, whether via a company issued or personal device, are both legitimate and secure.

Small wonder, then, why worldwide spending on information security and risk management technology and services is forecast to grow 12.4% to reach $150.4 billion in 2021: indeed, 61% of the 2,000 CIOs surveyed expected to increase cybersecurity spending in 2021[9].

The solutions and services currently available to combat hackers and safeguard digital activities fall into four broad categories:

1. Data centres security – According to the latest IDC-MarketScape report on[10] the colocation and interconnection services market, the data centre segment has performed above the average IT level over the past 18 months, buoyed by the demand for digital platforms driven by the Covid-19 pandemic. The report recognises Equinix and Digital Reality Trust as being two providers that offer multilayer portfolios that meet both current and emerging digital infrastructure requirements for most companies.
2. Cybersecurity software and services – One of the leaders in the field is California-headquartered Zscaler. Its cloud security model is designed for the cloud and mobility apps, enabling it to be deployed anywhere an organization has resources – including home offices. The firm offers a zero-trust exchange, where its cloud acts as a centralized hub for resources to connect with one another: applications protected behind the zero-trust exchange are not visible and cannot be discovered, thus eliminating the attack surface. Another market leader is New York-headquartered Varonis, which provides a security software platform to let organizations track, visualize, analyse and protect their unstructured data. The firm performs User Behaviour Analytics to identify abnormal behaviour and defend enterprise data from cyberattacks. Its software extracts metadata from an enterprise's IT infrastructure and uses this information to map relationships among employees, data objects, content, and usage - giving organizations more visibility into their data, and protecting their critical and sensitive information.
3. Cybersecurity chips – For many years, California-headquartered Nvidia has been supplying the GPUs (graphics processing units) used in data centres and supercomputers to power 3D simulations. But in 2021 it announced that it was breaking into the server CPU (computer processing unit) market with a new chip built on the ARM architecture. The CPU, codenamed Grace, won't arrive until early 2023. But Nvidia claims the chip will deliver 10 times the performance over the leading x86 server chips when it comes to AI and large-scale data science workloads. Some have speculated that the product may pose a competitive threat to Intel, which has long dominated the server chip market[11].
4. Cyber insurance – The global cyber insurance market is deemed to reach $24,185.3 million by 2025, according to estimates from Market Research Future (MRFR) in its 2020 report[12]. The demand for cyber insurance services is expected to soar during the forecast period (2020-2027) owing to adoption of blockchain and risk analytics software. Risk analytics are used by underwriters for assessing the valuation of premiums on digital assets and solutions. The faster speed of transactions and settlements without any middleman can facilitate the demand. In addition, the demand for first party coverage by insurers owing to larger presence online can drive the global cyber insurance market. London-headquartered insurance specialist Beazley is one of the market leaders.

Worldwide spending on information security and risk management technology and services is forecast to grow **12.4%** to reach **$150.4 billion** in 2021: indeed, **61%** of the **2,000 CIOs** surveyed expected to increase cybersecurity spending in 2021[9].

Sizing the opportunity

It's difficult to appreciate the full scale of the opportunity as it is still nascent and very few companies communicate on OT or have dedicated solutions for OT.

Indeed, connecting an operating apparatus to a network is the same as connecting any device. The zero-trust architecture does not care about the kind of device that is connecting to the network. What matters is the identity behind the device.

Endpoint security solutions will focus on OT while edge computing is still developing and needs specific security solutions. Edge computing is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed to improve response times and save bandwidth.

It's the opposite of the centralized full cloud model – and it will grow in tandem with the development of IoT and connected OT. That said, Crowdstrike, the world leader in endpoint solutions, estimates its total addressable market will reach $106 billion by the end of 2025, versus $36 billion in 2021.

Investing in tomorrow's world, today

While we are clearly entering a new phase in the evolution of cybersecurity that bears on little resemblance to what it was just a decade ago, from an investment standpoint we have to remember that the drivers that underpin this evolution are no different. They can be broadly described by digitalisation, innovation, regulation and globalisation.

What is different is the pace of change at which these drivers can accelerate and disrupt growth in markets and companies. There will always be companies that will miss the next opportunity and go from innovator to a legacy provider – the famous 'technology trap' that has ensnared many a company, perhaps most infamously, Kodak.

Furthermore, the shift from perimeter-based IT security to the cloud has brought about completely different challenges and associated technologies.

Staying up-to-date with the latest innovations and being curious about what might be the next direction for cybersecurity is therefore essential.

With the pandemic having an additional impact and shift to ways of working, this has only added to the pace of change. Companies and governments have a major role to play in bridging the cybersecurity gap for critical infrastructure and it needs to happen fast. This will also extend beyond simply protecting against a hack or a breach in the first place, but also developing stricter and coordinated plans and policies to determine what action to take when a breach or hack does occur.

In 2021, we've witnessed cybersecurity breaches of the Colonial pipeline, the largest fuel pipeline in the US as well as the world's largest food producer JBS Foods. In both instances, the firms paid ransoms to the hackers – $4 million in the case of Colonial[13] and $11 million in the case of JBS Foods[14].

The paying of a ransom is the least desirable of outcomes. As former FBI special agent and cybersecurity expert Jeff Lanza puts it, "*Do not pay the ransom for three reasons. Number one, you are not guaranteed you are going to get your information and the encryption key back. Generally, you will, but there is no guarantee. Second, if you pay, you are tagged as a payer, and you might get hit again. Third, a lot of times when someone pays ransom, that money can be used to fund other criminal activities – like human trafficking and terrorism activities – and criminals generally generate money to fund big operations by doing ransomware attacks. So you may be encouraging other illegal activity by paying ransom.*"

Of course, once the cybersecurity gap is closed for critical infrastructure, the nature of the industry means that there will already be another surfacing somewhere else in cyberspace. This makes cybersecurity – like the safety of governments, individuals and corporations more generally – a perennial theme in our lives and in our investments.

> Do not pay the ransom for three reasons. Number one, you are not guaranteed you are going to get your information and the encryption key back. Generally, you will, but there is no guarantee. Second, if you pay, you are tagged as a payer, and you might get hit again. Third, a lot of times when someone pays ransom, that money can be used to fund other criminal activities – like human trafficking and terrorism activities – and criminals generally generate money to fund big operations by doing ransomware attacks. So you may be encouraging other illegal activity by paying ransom.
>
> **Jeff Lanza,** former FBI special agent and cybersecurity expert

REFERENCES

1. Source: https://www.industryweek.com/technology-and-iiot/media-gallery/21962962/11-biggest-industrial-cyberattacks-so-far-slideshow/slideshow?slide=1

2. Source: https://www.dpstele.com/blog/major-scada-hacks.php

3. Source: https://www.dpstele.com/blog/major-scada-hacks.php

4. Source: https://www.cbronline.com/cybersecurity/top-5-infrastructure-hacks/

5. Source: https://www.industryweek.com/technology-and-iiot/article/21960609/manufacturers-of-medical-devices-warned-about-hacking

6. Source: https://oig.nasa.gov/audits/reports/FY17/IG-17-011.pdf

7. Source: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/a%20manufacturers%20guide%20to%20generating%20value%20at%20scale%20with%20iiot/leveraging-industrial-iot-and-advanced-technologies-for-digital-transformation.pdf

8. Source: https://www.cisco.com/c/en_uk/products/security/ciso-benchmark-report-2020.html

9. Source: https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-management

10. Source: https://www.equinix.se/resources/analyst-reports/interconnection-colocation-equinix-idc-marketscape

11. Source: https://www.pcmag.com/news/nvidia-unveils-a-cpu-chip-for-data-centers-supercomputers

12. Source: https://www.globenewswire.com/news-release/2021/06/14/2246715/0/en/Cyber-Insurance-Market-Valuation-to-Reach-USD-24-185-3-Million-by-2025-with-28-61-CAGR-IT-and-Telecom-Sector-is-Expected-to-Register-33-24-CAGR-by-2025.html

13. Source: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?sref=ialMV164

14. Source: https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781

NATIXIS
INVESTMENT MANAGERS

Additional Notes

This material has been provided for information purposes only to investment service providers or other Professional Clients, Qualified or Institutional Investors and, when required by local regulation, only at their written request. This material must not be used with Retail Investors.

In the E.U. (outside of the UK and France): Provided by Natixis Investment Managers S.A. or one of its branch offices listed below. Natixis Investment Managers S.A. is a Luxembourg management company that is authorized by the Commission de Surveillance du Secteur Financier and is incorporated under Luxembourg laws and registered under n. B 115843. Registered office of Natixis Investment Managers S.A.: 2, rue Jean Monnet, L-2180 Luxembourg, Grand Duchy of Luxembourg. Italy: Natixis Investment Managers S.A., Succursale Italiana (Bank of Italy Register of Italian Asset Management Companies no 23458.3). Registered office: Via San Clemente 1, 20122 Milan, Italy. Germany: Natixis Investment Managers S.A., Zweigniederlassung Deutschland (Registration number: HRB 88541). Registered office: Im Trutz Frankfurt 55, Westend Carrée, 7. Floor, Frankfurt am Main 60322, Germany. Netherlands: Natixis Investment Managers, Nederlands (Registration number 50774670). Registered office: Stadsplateau 7, 3521AZ Utrecht, the Netherlands. Sweden: Natixis Investment Managers, Nordics Filial (Registration number 516405-9601 - Swedish Companies Registration Office). Registered office: Kungsgatan 48 5tr, Stockholm 111 35, Sweden. Spain: Natixis Investment Managers, Sucursal en España. Serrano n°90, 6th Floor, 28006, Madrid, Spain. Belgium: Natixis Investment Managers S.A., Belgian Branch, Gare Maritime, Rue Picard 7, Bte 100, 1000 Bruxelles, Belgium.
In France: Provided by Natixis Investment Managers International – a portfolio management company authorized by the Autorité des Marchés Financiers (French Financial Markets Authority - AMF) under no. GP 90-009, and a public limited company (société anonyme) registered in the Paris Trade and Companies Register under no. 329 450 738. Registered office: 43 avenue Pierre Mendès-France, 75013 Paris.
In Switzerland: Provided for information purposes only by Natixis Investment Managers, Switzerland Sàrl, Rue du Vieux Collège 10, 1204 Geneva, Switzerland or its representative office in Zurich, Schweizergasse 6, 8001 Zürich.
In the British Isles: Provided by Natixis Investment Managers UK Limited which is authorised and regulated by the UK Financial Conduct Authority (register no. 190258) - registered office: Natixis Investment Managers UK Limited, One Carter Lane, London, EC4V 5ER. When permitted, the distribution of this material is intended to be made to persons as described as follows: **in the United Kingdom:** this material is intended to be communicated to and/or directed at investment professionals and professional investors only; **in Ireland:** this material is intended to be communicated to and/or directed at professional investors only; **in Guernsey:** this material is intended to be communicated to and/or directed at only financial services providers which hold a license from the Guernsey Financial Services Commission; **in Jersey:** this material is intended to be communicated to and/or directed at professional investors only; **in the Isle of Man:** this material is intended to be communicated to and/or directed at only financial services providers which hold a license from the Isle of Man Financial Services Authority or insurers authorised under section 8 of the Insurance Act 2008.
In the DIFC: Provided in and from the DIFC financial district by Natixis Investment Managers Middle East (DIFC Branch) which is regulated by the DFSA. Related financial products or services are only available to persons who have sufficient financial experience and understanding to participate in financial markets within the DIFC, and qualify as Professional Clients or Market Counterparties as defined by the DFSA. No other Person should act upon this material. Registered office: Unit L10-02, Level 10 ,ICD Brookfield Place, DIFC, PO Box 506752, Dubai, United Arab Emirates
In Japan: Provided by Natixis Investment Managers Japan Co., Ltd. Registration No.: Director-General of the Kanto Local Financial Bureau (kinsho) No.425. Content of Business: The Company conducts investment management business, investment advisory and agency business and Type II Financial Instruments Business as a Financial Instruments Business Operator.
In Taiwan: Provided by Natixis Investment Managers Securities Investment Consulting (Taipei) Co., Ltd., a Securities Investment Consulting Enterprise regulated by the Financial Supervisory Commission of the R.O.C. Registered address: 34F., No. 68, Sec. 5, Zhongxiao East Road, Xinyi Dist., Taipei City 11065, Taiwan (R.O.C.), license number 2020 FSC SICE No. 025, Tel. +886 2 8789 2788.
In Singapore: Provided by Natixis Investment Managers Singapore Limited (company registration no. 199801044D) to distributors and institutional investors for informational purposes only.
In Hong Kong: Provided by Natixis Investment Managers Hong Kong Limited to institutional/ corporate professional investors only.
In Australia: Provided by Natixis Investment Managers Australia Pty Limited (ABN 60 088 786 289) (AFSL No. 246830) and is intended for the general information of financial advisers and wholesale clients only .
In New Zealand: This document is intended for the general information of New Zealand wholesale investors only and does not constitute financial advice. This is not a regulated offer for the purposes of the Financial Markets Conduct Act 2013 (FMCA) and is only available to New Zealand investors who have certified that they meet the requirements in the FMCA for wholesale investors. Natixis Investment Managers Australia Pty Limited is not a registered financial service provider in New Zealand.
In Latin America: Provided by Natixis Investment Managers S.A.
In Uruguay: Provided by Natixis Investment Managers Uruguay S.A., a duly registered investment advisor, authorised and supervised by the Central Bank of Uruguay. Office: San Lucar 1491, Montevideo, Uruguay, CP 11500. The sale or offer of any units of a fund qualifies as a private placement pursuant to section 2 of Uruguayan law 18,627.
In Colombia: Provided by Natixis Investment Managers S.A. Oficina de Representación (Colombia) to professional clients for informational purposes only as permitted under Decree 2555 of 2010. Any products, services or investments referred to herein are rendered exclusively outside of Colombia. This material does not constitute a public offering in Colombia and is addressed to less than 100 specifically identified investors.
In Mexico: Provided by Natixis IM Mexico, S. de R.L. de C.V., which is not a regulated financial entity, securities intermediary, or an investment manager in terms of the Mexican Securities Market Law (Ley del Mercado de Valores) and is not registered with the Comisión Nacional Bancaria y de Valores (CNBV) or any other Mexican authority. Any products, services or investments referred to herein that require authorization or license are rendered exclusively outside of Mexico. While shares of certain ETFs may be listed in the Sistema Internacional de Cotizaciones (SIC), such listing does not represent a public offering of securities in Mexico, and therefore the accuracy of this information has not been confirmed by the CNBV. Natixis Investment Managers is an entity organized under the laws of France and is not authorized by or registered with the CNBV or any other Mexican authority. Any reference contained herein to "Investment Managers" is made to Natixis Investment Managers and/or any of its investment management subsidiaries, which are also not authorized by or registered with the CNBV or any other Mexican authority.

The above referenced entities are business development units of Natixis Investment Managers, the holding company of a diverse line-up of specialised investment management and distribution entities worldwide. The investment management subsidiaries of Natixis Investment Managers conduct any regulated activities only in and from the jurisdictions in which they are licensed or authorized. Their services and the products they manage are not available to all investors in all jurisdictions. It is the responsibility of each investment service provider to ensure that the offering or sale of fund shares or third party investment services to its clients complies with the relevant national law.

The provision of this material and/or reference to specific securities, sectors, or markets within this material does not constitute investment advice, or a recommendation or an offer to buy or to sell any security, or an offer of any regulated financial activity. Investors should consider the investment objectives, risks and expenses of any investment carefully before investing. The analyses, opinions, and certain of the investment themes and processes referenced herein represent the views of the portfolio manager(s) as of the date indicated. These, as well as the portfolio holdings and characteristics shown, are subject to change. There can be no assurance that developments will transpire as may be forecasted in this material. The analyses and opinions expressed by external third parties are independent and does not necessarily reflect those of Natixis Investment Managers. Past performance information presented is not indicative of future performance.

Although Natixis Investment Managers believes the information provided in this material to be reliable, including that from third party sources, it does not guarantee the accuracy, adequacy, or completeness of such information. This material may not be distributed, published, or reproduced, in whole or in part.

All amounts shown are expressed in USD unless otherwise indicated.

Thematics Asset Management is an affiliate of Natixis Investment Managers

THEMATICS ASSET MANAGEMENT

A French société par actions simplifiée (simplified joint-stock company) with a share capital of 191,869 €
843 939 992 Paris Corporate and Trade Register.
Approved by the Financial Market Authority (AMF in its French acronym) under number GP 19000027.
20, rue des Capucines – 75002 Paris
www.thematics-am.com

NATIXIS INVESTMENT MANAGERS

Paris Corporate and Trade Register 453 952 681
Capital : €178 251 690
43 avenue Pierre Mendès-France, 75013 Paris
www.im.natixis.com