Forging a new digital security paradigm

Global opinion paper

Atos

Contents

This opinion paper aims to provide an engaging and informed view of the key challenges that will shape the future of digital security. It explores in particular the main topics organizations should address to raise the bar in cybersecurity and win the cyberrace.

Cyril Dujardin,
SEVP, Head of Digital Security,
Atos

The digital and physical worlds are experiencing a complete disappearance of boundaries with digital becoming an integral part of our lives: in the objects within our homes, the utilities we use, the mode of transport we take, our workplaces and even, in some cases, augmenting our bodies.

In terms of digital security, there are no longer any boundaries either. Threats come from a wide variety of different actors from criminals to state-sponsored and everywhere in between. Motives are fluid from financial to geopolitical and anyone can be targeted from any location across the globe. Digital security threats can impact our physical safety, the security of our nations and our borders.

There are no boundaries between what must be protected by private and public sector: banks, power plants and transportation and logistics systems require the same level of critical protection as defense and emergency services. We have already witnessed devastating threats against civilians through attacks on power plants and water boards and we have seen warfare supported by cyberattacks.

Across industry, electronics and IoT devices are digitally embedded leaving them vulnerable to attack. The car you drive can be accessed and controlled remotely. All these systems must be protected.

As this blurring of boundaries intensifies, so too does the need to find ways to shape, protect and secure this digital dimension. Sovereign borders become more important as the desire for a globalized economy butts up against the need for protection of citizens, creating somehow a paradox between security and digitalization.

A tapestry of regulations and legislations are forming across the globe, a key requirement in enabling us to shape a digital world where the trust of citizens is the most precious commodity. In this context our mission is now to provide global holistic security across public and private sector organizations worldwide while addressing sovereignty concerns.

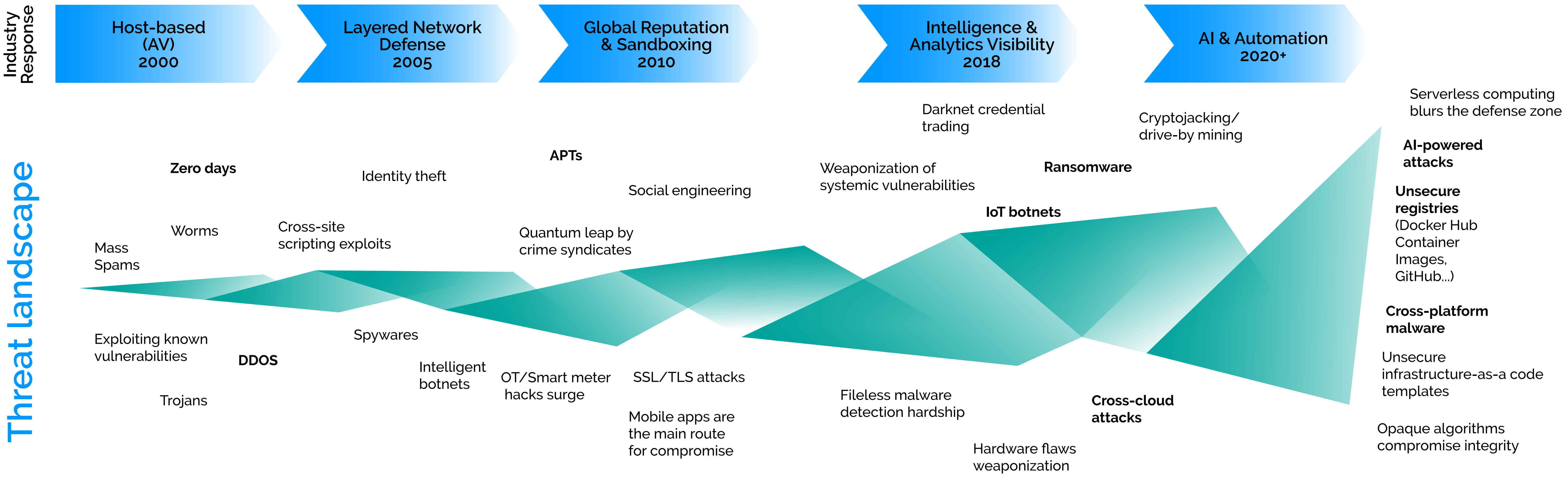
The success of digital security will define the world for the next decades. Will we live in a "big brother" world, where we have given up any willingness to control our data, our digital world and lives? Or will we live in a pacified world, based on trust, inclusiveness, and innovation?

Digital advancements must have the necessary controls, management of personal data and standardization of ethics in design to continue to be a force for good. Awarness of the security issue is growing, and global efforts are now falling into place.

Atos will stand alongside governments as a trusted partner, as well as a supplier of global solutions and of sovereign technologies.

Watch our videos and find out more at
atos.net/en/solutions/cyber-security

The need for a new digital security paradigm



Industry Response

Host-based (AV) 2000

Layered Network Defense 2005

Global Reputation & Sandboxing 2010

Intelligence & Analytics Visibility 2018

AI & Automation 2020+

Threat landscape

Mass Spams

Zero days

Worms

Exploiting known vulnerabilities

DDOS

Trojans

Cross-site scripting exploits

Identity theft

Spywares

Intelligent botnets

APTs

Quantum leap by crime syndicates

OT/Smart meter hacks surge

Social engineering

SSL/TLS attacks

Mobile apps are the main route for compromise

Weaponization of systemic vulnerabilities

Darknet credential trading

Fileless malware detection hardship

IoT botnets

Ransomware

Hardware flaws weaponization

Cryptojacking/ drive-by mining

Cross-cloud attacks

Serverless computing blurs the defense zone

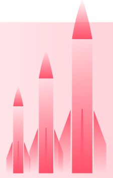
AI-powered attacks

Unsecure registries (Docker Hub Container Images, GitHub...)

Cross-platform malware

Unsecure infrastructure-as-a code templates

Opaque algorithms compromise integrity



Cyber Attacks More Likely to Bring Down F-35 Jets Than Missiles

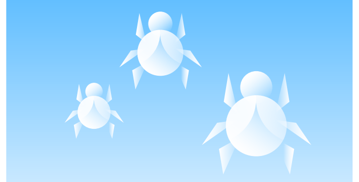
Cybercrime To Cost The World $10.5 Trillion Annually By 2025

(Source :RiskIQ)

> More than 90 percent of all healthcare organizations reported at least one security breach in the last three years.
>
> (beckershospitalreview.com)

Malware increased by **358%** in 2020

(Source study by Deep Instinct)



February 2021

Cyberattack against a water system in Florida exposes system to water water poisoning

February 2021

Bombardier suffers cyberattack

February 2021

French hospitals hit by cyberattacks

March 2021

Exploit of a vulnerability in Microsoft Exchange Server leads to data breach - Belgium's interior ministry announces it was hacked

May 2021

Ransomware Attack on the Colonial Fuel Pipeline

An ever more prolific threat landscape and how to fight back

by Lukasz Olszewski, former Global Head of CERT, Atos

The cyberthreat landscape is increasingly prolific, sophisticated and tricky to defend against. Much of this is due to a rise in state-sponsored attacks, for-hire cybercriminals and rapidly evolving offensive technologies. These add additional complexity around issues of data sovereignty and control. This is pulling the private and public sector closer together and further cooperation is needed to tackle what is at stake.

A fundamental part of the problem is the motive, opportunity, impunity cycle where we see high rewards and minimal punishments in cyberattacks. This is exacerbated by state espionage and cyber warfare, which prevents global consensus in tackling the issue.

There must be a step change in how public and private sector work together across the globe to manage cyber threats as the economic and political risk involved increases year-on-year, not to mention the risk to public safety and global geopolitics.

Impunity

Part of the issue is that threat actors can feel protected by their governments when there aren't any co-operations in place for prosecution and where state-sponsored cyber warfare muddies the water. But what is also at stake is a lack of resources and skills to tackle cybercrime globally and, in some instances, a lack of political will.

Unless governments and private sector tackle this as a global crisis – all working together – there will be little change in the proliferation of attacks.

Obviously, cybercrime is remote: a threat actor may be sitting in one country attacking an organization or government in another feeling secure in the knowledge that it is highly likely he will not be punished. Being able to act with impunity means there is really no deterrent at work.

Motive

The other major issue in cybercrime more specifically are the financial benefits. The US Department of Justice said it had recovered $2.3 million worth of Bitcoin that Colonial Pipeline paid to ransomware extortionists .

Ransomware is now a huge issue for organizations and, perhaps more dangerously, for public sector and critical infrastructure. If an attack puts people or an organization at risk, the policy is generally to pay the ransom and resume services or safeguard operations as swiftly as possible.

There is never any guarantee when paying a ransom that you will be safe afterwards. There is little honor among criminals, and so it is becoming increasingly common for criminals to use the same attack method more than once – they had success the first time and a few weeks later may try again. They can be successful on more than the first occasion.

Moves are being made, particularly in the US, to make the payment of ransoms difficult for organizations and reduce the amount of money going to organized criminals. Broadly, more input from government on tackling this issue is welcome, but criminalizing organizations for payment needs to be balanced with more practical support to help organizations recover quickly from an attack – this element is still lacking in legislative approaches thus far.

With the above cycle still playing out, what can we do to protect organizations?

Cybersecurity teams keep getting better at tackling cybercrime, says Maciej Zarski , Global Head of CERT, Atos, "The threat landscape is slightly changing every year with new TTPs (Tactics, Techniques, and Procedures) but we still observe that the basic threats are very effective, including: phishing, stolen credentials, ransomware, poor security hygiene and DDoS, DoS. This means we can hunt, detect, plan and educate against these threats. However, tackling the root cause – breaking the impunity cycle – must be the long-term goal.

To break this impunity cycle what matters is accountability. Even if it does not solve the problem completely, surely it should slow down cybercrime."

[1] https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

> Some of the most destructive and costly ransomware groups are now in their third incarnation over as many years.
>
> **Brian Krebs**
> American journalist and investigative reporter
> **from Krebs on Security**

When two worlds collide: The uncomfortable convergence of IT and OT environments

By Eyal Asila, Head of Digital Cyber Consulting, Atos

The fourth industrial revolution has seen two different domains – IT and OT – forced together, causing a convergence that benefits industry and consumers but can also leave operations, sometimes critical operations, open to risk.

Learning to manage the risks and understanding how critical this is will enable further digital transformation and, importantly, safeguard citizens and economies.

Not designed to be connected

The OT environment was not originally designed to be connected. In many cases, the OT environment is extremely expensive to build and complex to change . It does not run on the same operating systems used in a modern technology environment and does not easily lend itself to upgrade and adaptation.

For this reason, when the two environments converge, a potential major cyber risk is introduced, and this must be managed. Regulators and governments are now increasingly aware of the risks and seeking to ensure industrial organizations manage and control it. Many critical infrastructures: utilities, logistics, healthcare, and more, are based on these complicated systems.

Across the globe we have seen cyber criminals and threat actors use these vulnerabilities for ransomware attacks and cyber warfare which, in the worst cases, have put people's lives at risk, changed economic situations and even introduced a strategic game-changing factor to international government relationships and warfare.

Knowledge gap

One of the key issues in this area is the huge knowledge gap in the market. This is an extremely specialized area, and it is rare that you have professionals with expertise in both IT and OT security.

I am aware of an incident, where an expert insisted that an HMI (Human Machine Interface) in a production line be shut down due to a minor security breach. What he did not know was that this single HMI was critical to business operations and also under the control of regulators. The entire production stopped needlessly and could not run again until the regulator had approved the process, this took more than six months.

Understanding processes, people, and organization

For this reason, the first step Atos takes when looking at securing a complex environment is developing a deep understanding of the entire environment and business processes, including what is being produced and why. Indeed, it is essential to ensure that everyone working and operating machinery or systems within the process has a clear view of the end-to-end business, especially what in the process is critical – which machine is their crown jewel.

This information ensures a correct assessment of the risk as well as of the daily operations; it also supports the incident response process and allows the organization to minimize its risk exposure.

Moving on to defining each components' capabilities is the next stage and then a full evaluation process is undertaken called the discovery phase. A deep dive into the overall converged environment that contains IT (including cloud, on-premises, third party, etc.) and OT assets. Running visibility and behavioral anomaly detection through the entire process and searching for any vulnerabilities means a well-defined mitigation program can be developed and put into action. Only once these steps are complete can the work begin to upgrade digital security.

For digital security, organizations need to:

- Understand what their security vulnerabilities are,
- Understand what impact should be expected if an attack were to occur,
- Decide what is critical to secure and how.

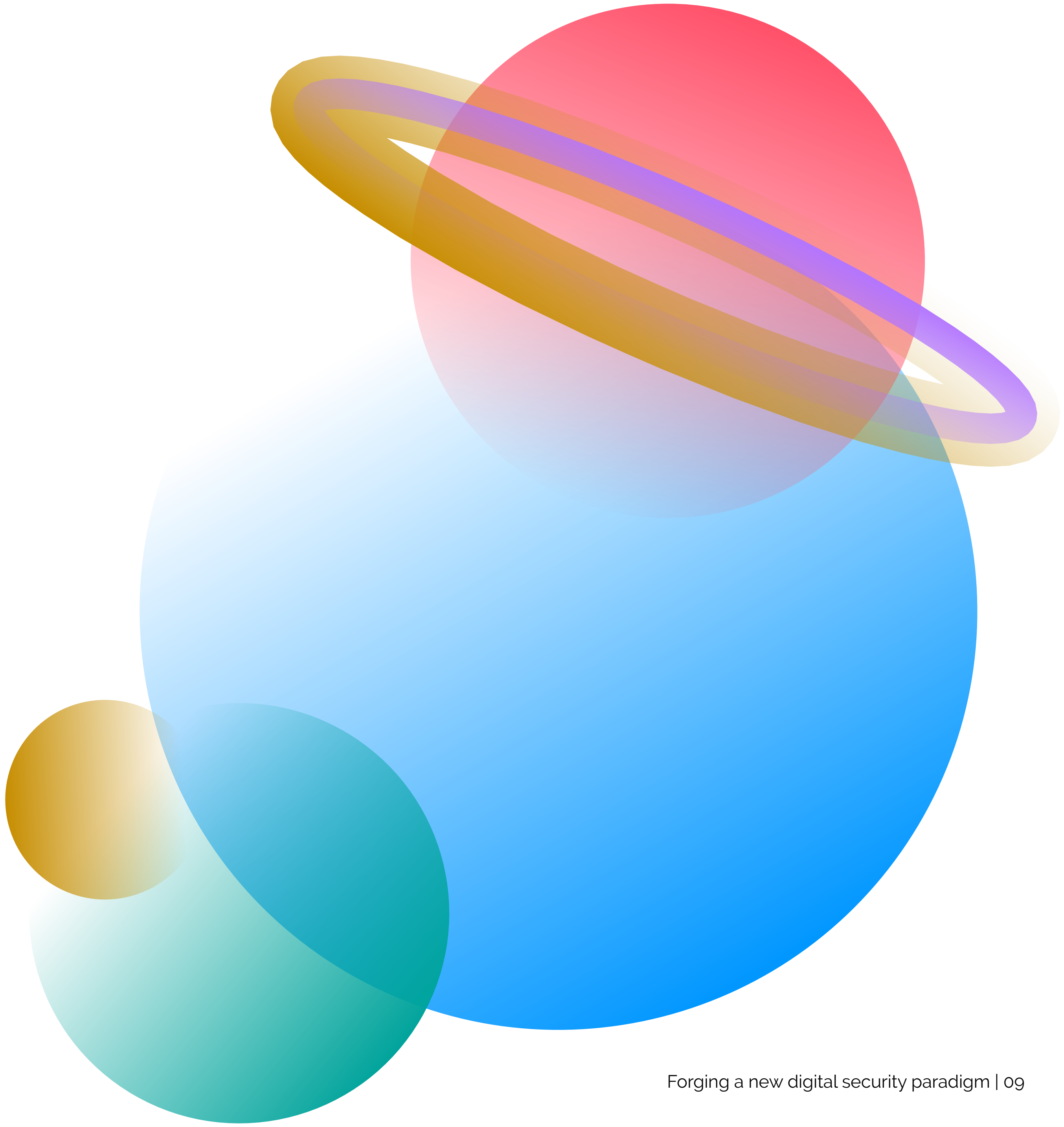
The solutions are not straight-forward in the OT environment – technology systems such as patch management, antivirus and updating operating systems are all irrelevant so bespoke solutions are often necessary. That is why Atos has invested in specialized tools and products for securing complex environments and ongoing threat detection and management to be able to address such specific challenges.

However, nothing can be done without the proper risk management strategy at its core. It is therefore crucial for organizations to put a strategy in place. This should cover all relevant areas such as policies, procedures, and processes, including any incident response plans that need to be in place and training people in the management and detection of risks.

The work is in progress, but it needs to go faster.

> Extreme environments call for extremely reliable communication solutions and we were looking for a French specialist to help coordinate and secure our first offshore wind farm in France. The experience of the Atos teams, their knowledge of offshore and the very specific digital and OT technologies associated with this area are very valuable to us.

Javier Garcia Perez
President of **Ailes Marines**
International Offshore Director of **Iberdrola**
https://atos.net/en/2020/press-release_2020_12_01/ailes-marines-offshore-wind-farm



What does data sovereignty mean for the enterprise?

By Vasco Gomes, Global Chief Technology Officer for Cybersecurity Products, Atos

Data sovereignty has become the new buzzword in managing the digital economy, globalization and geopolitical influence.

But, as states begin to wrangle over big tech power and control, do we really understand what data sovereignty means and how it translates to the enterprise?

Data sovereignty for the enterprise

Historically, the sovereignty adjective was used in relation with states and political power. When using it for enterprise data, it becomes trickier to define and understand, particularly in our new globalized economy.
There is still no standardized or clear definition, particularly for an enterprise. The most accurate description is the degree of control an individual, organization or government has over the data they generate and work with. For this reason, data sovereignty is non-binary. It exists on a scale and that scale is constantly in flux. It is also inextricably linked with security and requires a technological response.

Macro influencing micro

We can see data sovereignty issues at play on a macro level with some governments sanctioning the use of certain technology providers due to concerns for national security, including fear of sensitive or classified data leakage. When there is a risk of commercial warfare and state espionage, then the provenance of the solutions used for protecting data becomes a critical question. If you cannot trust the microprocessors processing your data in your hardware because they are made elsewhere, you can see that the issue of sovereignty and security becomes extremely tricky. And when the functioning of critical sectors, from a hospital to a gas pipeline, depends on resilience of its digital infrastructure or access to data, technological choices become strategic. However, there is no single organization across the globe who has that capability to build and produce all aspects of their supply chain. So where do we go from here?

Whatever the future holds, identities and encryption are key

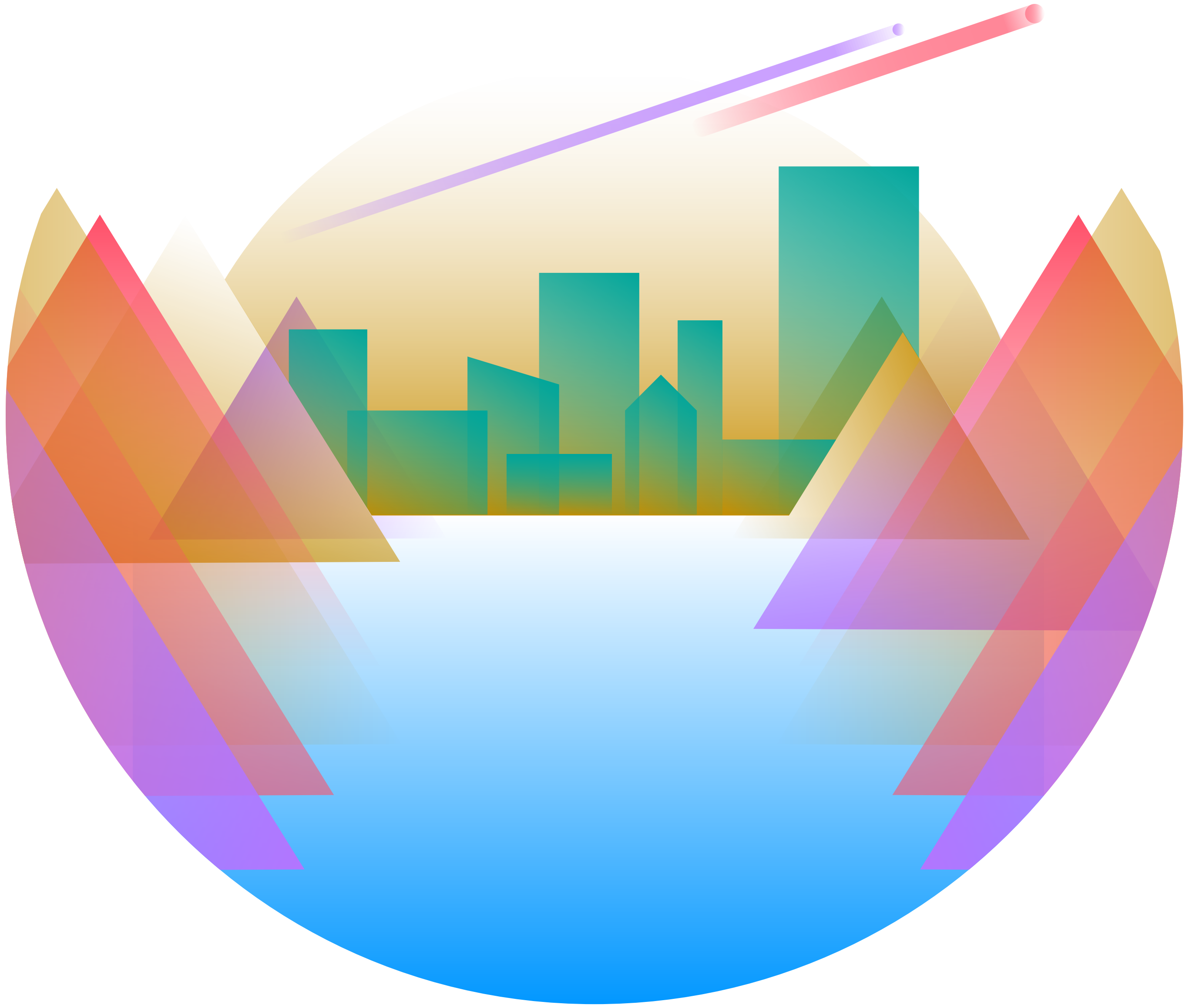
Different technological domains provide different levers to influence the degree of control an organization has over data, whether it is data the organization generated or acquired or is entitled to use. As data gains value through its usage, how it is stored and computed are critical, but cannot be the only levers to consider.
Organizations who want to maximize their data sovereignty will also need to pay particular attention to the control of data access and data usage.
For those objectives, while identities and encryption are obviously not the only controls to consider, they are paramount, universal and, we believe, whatever the future evolution of technologies, they will always remain of utmost importance to address cybersecurity and sovereignty challenges.

Managing what we don't know

The issue boils down to the question: *what don't we know?* The key is in ensuring an ongoing process of data classification and risk mitigation. Digital security, and therefore data sovereignty, must be driven by constant risk assessment: probability and impact; benefit for the business; list of mitigation actions with percentages. Decisions based on these assessments must be taken with all the information you can gather at the highest levels of any organization. The board can decide whether it wants to maintain, mitigate, share or avoid the security risk associated with any new technology or service.
I believe data sovereignty is a conversation about value versus risk: *where is the position with the maximum value for the minimum risk?* It is a decision we make constantly at all levels of society today: individuals, enterprises and governments. In some cases, for some technologies, there should be a clear no-go because those are critical assets for the enterprises.
It is the right conversation for our time, allowing us to focus on value while always understanding and minimizing risk. In this way, we can all progress within our new globalized economy.

[2] Crypto AG (2020) and NSA spying on European leaders with Denmark complacency (2021) https://www.bbc.com/news/world-europe-57311441

> This is not about turning our backs on partners. It's about having the courage to say that we don't want non-European law to apply to these services.
>
> **Guillaume Poupard**
> Director of the French Cybersecurity Agency on French proposal to prevent critical data from being accessed to by U.S authorities



When physical and digital worlds collide

By François Cortial, Chief Technology Officer, Mission-Critical Systems, Atos

At one point, the engineering world was binary, concerned with the designing and building of physical machines and structures. This is now blurred, with a digital profile that is changing the nature of engineering.

Cars are an excellent example of this changing profile, with Tesla CEO Elon Musk describing the Model S Tesla as a very sophisticated computer on wheels, back in 2015. Previously, they were physical machines operating an engine and wheels and built by systems engineers; nowadays they have all the digital intricacies of a computer working in tandem with a physical machine. In the future, it is likely that cars will be closer to a computer in terms of build than the cars of previous generations. So how do we protect against security risks in an interconnected world, where the boundaries between physical and digital are becoming more and more blurred?

Cybersecurity as part of dependability

Critical infrastructure protection is key to guarantee dependability of our vital assets. For example, energy plants, emergency and health services and state services cannot afford any failure or disruption. For a long time, dependability was considered in system engineering with a physical-oriented mindset, alongside Reliability, Availability, Maintainability, Safety (RAMS). We are now talking about cyber-physical systems (CPS) and so fault, incident, attack areas are both physical and digital. Cybersecurity is now part of dependability, and the two topics must be addressed jointly (RAMS+S).

Both systems engineers and cybersecurity experts must consider dependability and risk but, so far, there is no common language between the two disciplines and crossover is still rare. The two separate experts must work together to design systems that are both physically and digitally secure.

Assembly robots in factories, turbines and flow control in energy plants, railroad switches and traffic systems in railway companies, are often networked with supervisory control and data acquisition systems (SCADA), sometimes through time sensitive networks (TSN) and over remote sites. Any failure or intrusion in such systems can lead to subsequent disruption of service, and at worst to catastrophic events or disasters.

It is also important to think about communication technologies. In fact, connectivity is an intrinsic part of the digital world, and any malfunction in this area can lead to complete end user service disruption. This is the case for all communication systems deployed for the operation of critical infrastructures or public safety. For example, any outage (either physical or digital) in an emergency management system at a region or country level can lead to critical impacts, including endangerment of human life.

Keeping pace with evolving technologies

In this major movement, new technologies and implementations are appearing, making the problem even more complex. Software defined approaches, virtualization of hardware, edge and fog computing and artificial intelligence (AI) driven applications are becoming the new normal. Furthermore, all these new trends must get along with old legacy systems that have not been designed with these emerging technologies in mind and cannot be renewed simply.

Finding a solution

Building a solution that encompasses people, processes and technology must be at the heart of all operations. This means understanding both the physical and digital systems within the ecosystem and how they interact, and making security part of the culture of an organization and something everyone is responsible for.

Unfortunately, there is no perfect solution, and even less when complexity increases, reaching a system-of-systems level . Reaching operational safety within an acceptable risk profile can only be achieved by combining "by design" approaches and through continuous monitoring of the system during operation. Resilient systems that can automatically monitor themselves and flag any deviation from the expected quality of service and automatically apply countermeasures in an adaptive way.

At Atos, we would always recommend modern architectures, secured by design, and to set up collaborative mechanisms across different parts of a system. This is the best way to manage the risk of digital security incidents down to an appropriate level.

Unless security can be guaranteed to an appropriate level, complex systems such as autonomous cars cannot be used on a wide scale due to risk to life. Lack of security is a threat to technological progress.

[3] System of systems is when multiple different systems interact with each other to provide complex functionalities with increased efficiency.

> The security of our fans and their physical and online environments is of the utmost importance to us. While more than 65,000 fans are excited for touchdowns, most are unaware thousands of technology devices in our stadium's infrastructure must be protected from malicious intent by threat actors.
>
> **Kim Rometo**
> Vice President, Chief Information Officer,
> **Miami Dolphins and Hard Rock Stadium**

Digital security and public safety at a crossroads

By Eric Wahed, Global Head of Public Safety / NG112, Atos

As society becomes increasingly digitalized, safety and security in the real and digital worlds are increasingly intertwined. Digital can now support in the prevention, protection, detection, and response of real-world public safety threats. However, this opportunity requires careful management of public trust, data integrity and security. If security is breached and trust is squandered in this area, benefits and opportunities for greater public safety will be lost.

What you need is a contract between cities and citizens to help maintain the peace and keep each other safe. In this way, society is active in public safety and share data – both proactively and through consent – with emergency services and local government for the benefit of society and improved safety. We also need better data sharing between government and local agencies to provide better services, greater efficiencies and improved public safety.

Predictive policing

The making use of social and economic contextual data points can help to predict times of heightened safety concerns. For example, understanding when people are paid or when there are large sporting events taking place can help predict flashpoints for criminal behavior.

Predictive policing means that local government can offer its citizens the right support at the right time to avoid potential unrest. A broad view of potential flashpoints enables better and more proactive policing and decision-making. However, only with a trusted partnership in place between citizens and public sector, can public safety truly benefit from such developments.

Data sharing and network management in public safety

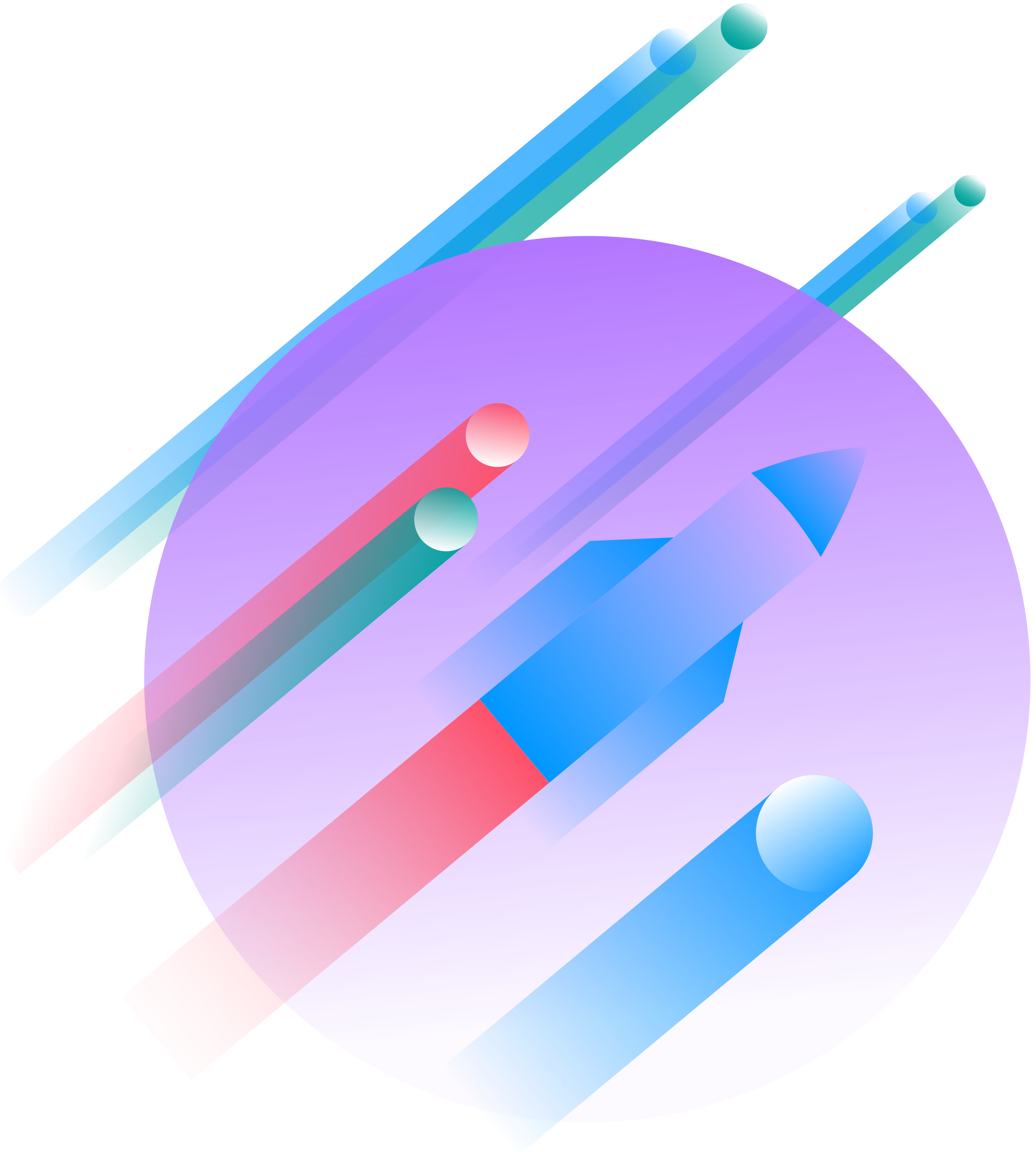
Enabling different agencies to share information and collaborate on incident response and information can be a real game-changer for public safety and is sadly still very rare — due to legacy IT systems and complexity around data protection. In Spain, Atos has developed a unique intelligence sharing system, the first of its kind, with an emergency response center that has representatives from emergency medical services, doctors and nurses, firefighters, Guardia Civil, national and local police. These agencies are set up in concentric circles to visually maximize collaboration. Between them, they can make appropriate decisions on how and who is best to respond to any given emergency. This integration of agencies provides increased agility and efficiency and, crucially, a better response and outcome for citizens.

This model can also work virtually, creating an ecosystem that shares various data points across different government agencies through new secure networks and data exchanges. These must be protected with identity and access management controls and the data must be encrypted on every step of the journey. These ecosystems can provide real-time data on contextual data points, incident response, and local government information on individuals. Atos has managed a system of this kind in the UK, identifying vulnerable citizens by sharing intelligence between five public service organizations in a county within Wales. The project aims to enhance the quality of response and enable more strategic assessments of the needs of vulnerable citizens, providing a service that can be both tailored and efficient.

Security and ethics

With an increasingly digitalized society, progress in data sharing and its use for public safety is inevitable, and will bring efficiencies as well as benefits. The process behind it, however, still needs to improve significantly.

I am optimistic this change will happen. Public trust will increase if citizens are kept aware, understand the process and can see it is transparent and brings personal and societal benefits. Building systems through the prism of digital security and ethics is vital.



Putting the business impact of cyberthreats on the board agenda

By Paul Bayle, Head of Security and CSO, Atos

Increasingly, the cybersecurity strategy for an organization must be baked into its business strategy to ensure that it can manage an increasingly complex digital environment.

Investment in security is vital for an organization, not only for maintaining security and trust of customers, but providing a competitive advantage and enabling long-term growth through secure digital transformation. Giving the board the right information at the right time is paramount in keeping cybersecurity on the agenda as a business benefit, rather than a cost.

Knowledge is power – inside and out

The conversation around budgeting for digital security must demonstrate a complete knowledge of the digital environment. This can be complex in large and distributed organizations where shadow IT and shifts in working arrangements may have changed the landscape incrementally. An understanding is needed of:

- The business imperatives
- Plans for the future
- Digital perimeter and assets
- Processes and people

This is not a straight-forward task, but shining a spotlight on how much there is to protect and the full scope and scale of the job at hand is essential.

Build a story that speaks to the board

Once this is established, it is time to look outside of the organization and ensure board awareness of the increasing rate of cyber threats. This can be achieved through regular reporting across competitors and the landscape. A regular feed of information on attacks and consequences – both reputational and financial – can help those who are not involved in security to understand the prevalence and level of business risk involved. Indeed, security metrics used by security practitioners (such as vulnerabilities or number of incidents) do not often speak to the board, as it is difficult to see their impact on the business.

Board interest centers around benchmarking security metrics with peers: *How does my organization's security compare to peers of similar size and in the same industry?* including benchmarking security spend as a percentage of IT budget, peer comparison on average incidents per high value assets, and peer comparison on average critical vulnerabilities per asset.

There is also growing recognition at the board level on criticality of response. As an example, the speed at which a business unit can be restored back to normal operations after a security incident or breach is a high value metric at board level. Investments and initiatives towards decreasing the time to bounce back to normal operations and lower business loss due to faster restoration is gaining high traction at board level in the context of the ever-increasing ransomware threat.

This information can be used to build a story that identifies the risks at the perimeter and the ways in which an organization is vulnerable. Ensuring this information is presented through business-driven metrics will enable buy-in. Aligning security metrics with Balanced Score Card methodology is an effective way to communicate to the board. Metrics that reflect the four areas of Balanced Scorecard (including financial, customer, operational, learning & growth) are simple and meaningful. From here, a plan and an appropriate budget can be formulated and the exercise is transparent and easily understood by all stakeholders.

What is the appropriate budget?

The issue for CISOs is that this question has no easy answer, the amount you could spend on security is almost limitless!

Even the most protected organizations could still have vulnerabilities, and an important balance must be struck between risk and reward. They must ensure that all known threats are covered and, importantly, that there are appropriate controls in place to detect threats before they become an issue and protect the organization from them.

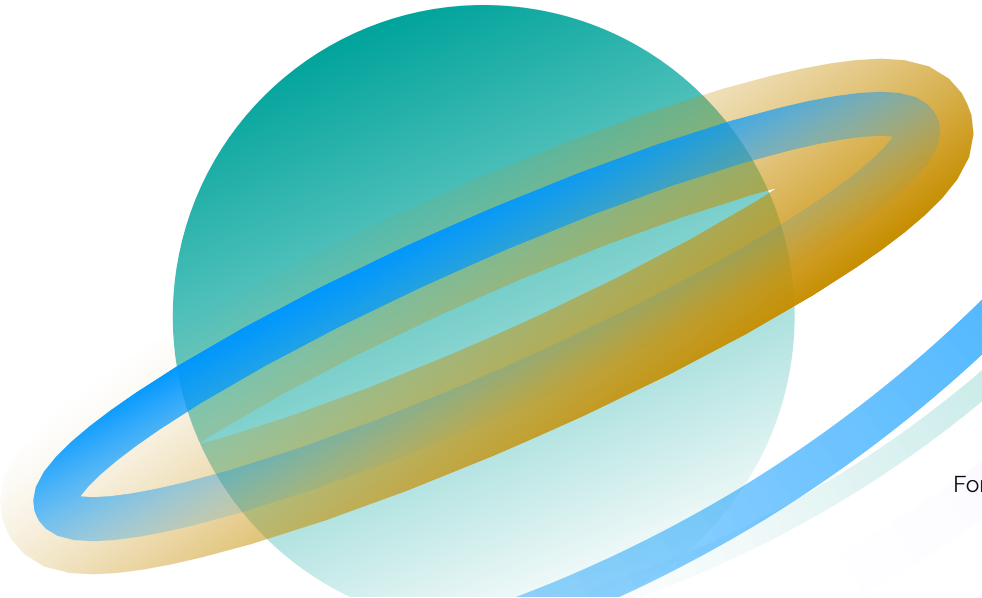
Although organizations share more than before on cybersecurity incidents, there is still reticence to disclose or talk openly about them. However, more transparency from organizations on the costs they have incurred from security breaches would be a helpful indicator on the level of budget that should be allocated for security. Public agencies such as the European Union Agency for Cybersecurity (ENISA) could support the private sector with this by collecting and anonymizing data.

External forces

Increasingly, legislation and regulations are forcing accountability for digital security up to the board level. Securing personal data and maintaining the security of critical infrastructure are public and private sector concerns with fines from authorities for any failure to secure data.

Insurance companies are also becoming wise to the potential costs from security issues and increasingly need to see detailed plans for cybersecurity to underwrite risk.

The bottom line is that organizations cannot sit still on this issue. The board needs to be kept informed of risks on a regular basis and understand that security is evolving quickly. Following numerous recent and successful ransomware attacks, threat actors have access to money and are extremely smart. Keeping up with them requires ongoing work, dedication and, importantly, investment.



The vital role of data protection within security strategies

By Deborah Dillon, Head of Protection and Privacy, Atos

Privacy functioning across disciplines

Personal data is now widely used by organizations across the public and private sector to provide better personalization of services and to give organizations competitive advantage. Because of this, protection of personal data has become a vital aspect of digital security in order to maintain the trust of consumers and citizens.

If consumers believe their data is not being appropriately managed, they could withdraw the right for organizations to use it. This debate is currently ongoing in the UK with patients now given the option by the National Data Guardian to opt out of sharing their data with the NHS. This move came as a result of citizens not trusting that the appropriate privacy measures were in place to secure their data and anxiety over its ability to be sold or shared with third parties.

Privacy must be considered as a vital ingredient to business strategy, which means it needs to be understood from board level to operations within an organization. It can no longer serve as a function that sits solely within legal and compliance, it must be cross-discipline and its importance must be understood by all.

Putting privacy at the heart

Understanding data classifications and how it must be stored and processed is a vital aspect of maintaining its integrity in accordance with privacy laws. This requires having the right processes, tools, and technologies in place to encrypt and safeguard to the right level.

The introduction of GDPR recognized that digital transformation brought increased complexity to the area of privacy and Article 32 requires Data Controllers and Data Processors to implement technical and organizational measures that ensure data security appropriate to the risk presented by processing personal data.

Privacy must be built into digital security planning with privacy by design principles in place and data privacy impact assessments as standard. There must be an awareness of what data is being held, how sensitive it is, and what the ramifications of any data breach would be. Under GDPR, there is a 72-hour timeframe in place for reporting a data breach to the Regulator. An understanding of what constitutes a serious data breach and what needs to be in place to manage any fallout should one occur needs to be in place, preferably at board level or with direct access to the board if necessary.

Scenario planning

For this, a data management playbook that roleplays the management of a serious data breach can be useful. You cannot wait until something happens. You need everything pre-prepared in your back pocket to manage any breach should it occur.

The hours following a breach are critical to organizations to limit any fall out and damage. Maintaining a relationship with consumers who are giving organizations access to their data is absolutely vital, knowing how and when to communicate is key.

There has been an increase in public prosecutions for data breaches and this has the potential to become a serious issue for organizations. Law firms have identified this risk as a new revenue stream and, in some instances, they are chasing and encouraging consumers to bring privacy cases against organizations.

The role of privacy in ethical design

Developing ethical frameworks and standards must be the next step in ensuring privacy laws are not only followed but also improved upon and future-proofed. This is particularly important as the use of technologies such as artificial intelligence (AI), machine learning (ML) and automation have the potential to unwittingly cause harm.

Atos leads the way in ethical design principles for digital, having enshrined the concept within its raison d'être. Working with competitors and the European Union on developing ethical frameworks for design is an ongoing workstream.

If you look at the origins of privacy, it was brought in after the Second World War to guard against abuses by any authoritarian regime. The right of citizens to know their data is not going to be used in a way that has the potential to harm them is vital. The data genie is out of the lamp, we cannot put it back, but we can guard against misuse of the power it brings.

> According to Gartner, privacy is no longer "just a part of" compliance, legal or auditing, privacy is becoming an increasingly influential, defined discipline of its own, affecting almost all aspects of an organization. As a rapidly growing stand-alone discipline, privacy needs to be more integrated throughout the organization.

[4]https://www.theguardian.com/society/2021/jun/06/the-nhs-data-grab-why-we-should-be-concerned-about-plans-for-gps-records

[5]https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

Security by design: bridging the gap between system engineering and cybersecurity

By François Cortial, CTO Mission critical systems, Atos

Security by design is a vital step in reaching operational safety in the convergence of physical and digital systems. This, alongside continuous monitoring during operation, is the best way to ensure resilience and security. However, even with modern architectures in place, it is not sufficient.

Experience demonstrates that once in operation, systems can evolve and go beyond the limits considered during the design phase. This is even more true in cybersecurity, where threats are continuously evolving, making what was planned at one point obsolete later.

Security by design includes continuous system monitoring

Continuous monitoring of systems is required to detect any deviation from what was planned, in terms of global wear and tear, achievement of the expected service, abnormal events, evolution of cyberthreats, and more. Such solutions can then raise alerts, or at the best, intermediate automatically by triggering maintenance operations, or interacting with the system in an adaptive manner (putting some new rules in the system configuration for example).

It is necessary, therefore, for security by design to also consider monitoring across the physical, digital and cybersecurity aspects of a system as part of the overall approach. A good example of where this is required is in the area of railways, where such system monitoring can be used to detect any event outside the planned domain of operation (considering the functional, environmental, cybersecurity aspects), with the goal of bringing any insufficiency or cyber attack into an acceptable and manageable risk zone.

Finding common ground between system engineering and cybersecurity

There is currently no common language for security and resilience between system engineering and cybersecurity. They are different disciplines with different expertise, skills sets and methodologies. On the physical side, there are plenty of structured approaches such as the Failure Mode Effects and Criticality Analysis (FMECA) and its enhanced variants, both in terms of hardware and software. But these methods do not take cybersecurity needs into consideration.

A good answer may be to lean on the [6]IEC standardization, especially the IEC 62443 and the part 3.2 about security risk assessment and system design. However, it is more a guidance about risk analysis and control than a structured method, like FMECA.

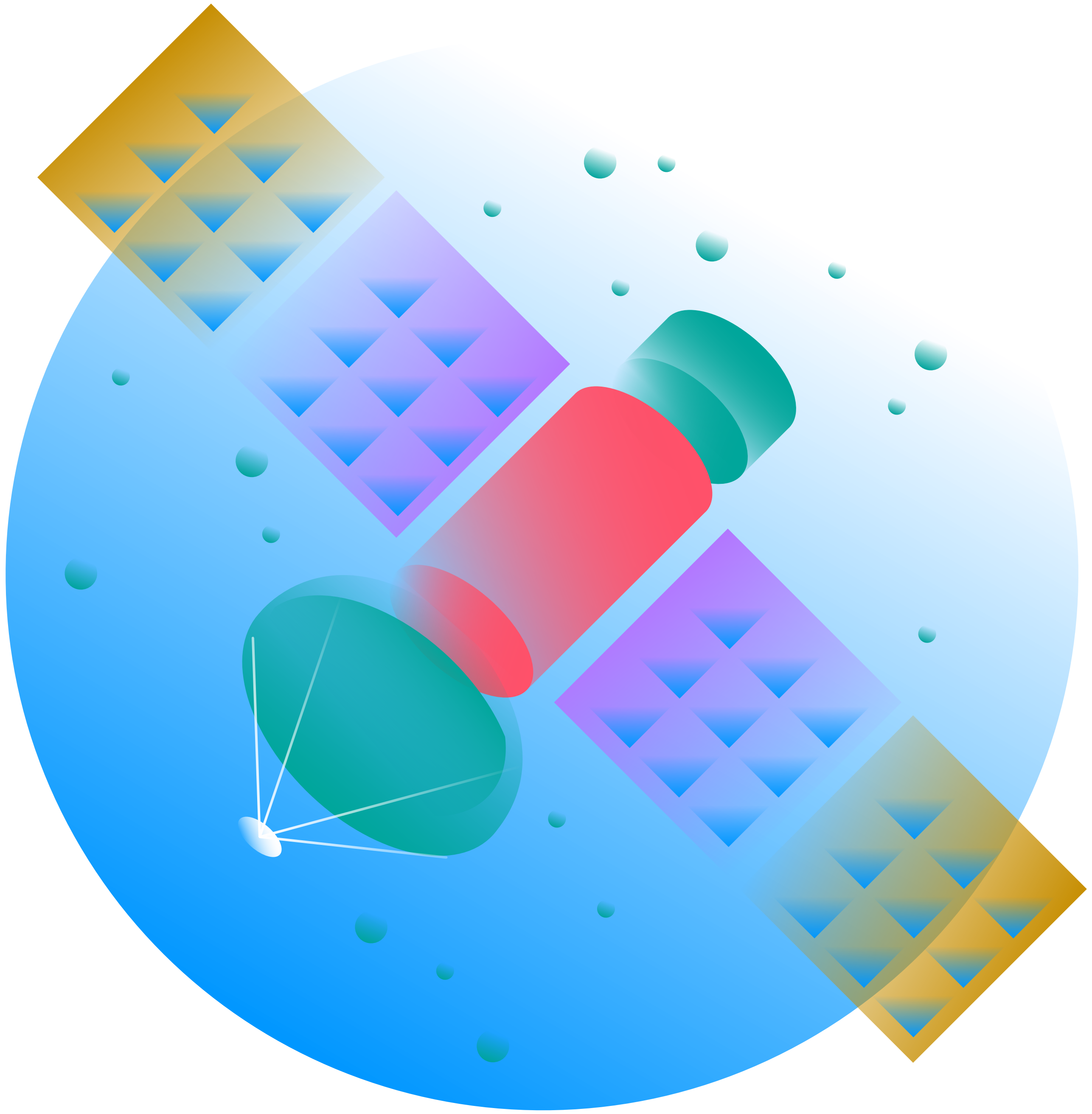
To carry out such analysis, current trends focus on systemic approaches, by breaking down the system and its environment into multiple elements, so that the behavior of each element can be modelled. It is then conceivable to execute a certain number of deviant scenarios, to assess the weaknesses and the failure mode propagation in the global system, on both physical and cybersecurity aspects.

Digital twin

Another step is to enhance the concept toward a digital twin of the live system. The interest here is to keep the system modelling alive besides the real system during its entire lifecycle, continuously improving the risk assessment by machine learning from the collected data of the real system.

Let's consider a very specific example, such as the testing of satellites. Satellites cannot afford any failure or misfunction after the launch, given the difficulty in correcting breakdowns or intrusions. A digital twin of the full system – satellite plus space check out equipment (SCOE) can carry out a virtual risk analysis, before the launch, and during the operational life to ensure any potential issues are flagged and fixed through predictive maintenance before any real-world breakdown occurs.

Security by design followed by continuous detection and response systems monitoring through AI and ML to find any anomalies in activity and user behavior is vital. Alongside this for the digital side of a system, a digital twin could be used to model the physical system and stress test it in an experimental environment. Creating resilient and secure cyber physical systems is extremely complex but two disciplines working in tandem can find solutions that work across a system for its entire lifespan.



[6] International Electrotechnical Commission

Shortage of cybersecurity skills, which way forward?

By Catalina Dodu, Global Presales Director for Cybersecurity Services, Atos

Attacks are increasing exponentially and are a reality for all individuals and companies. With ransomware as a service able to be bought on the dark web, anyone can be a cybercriminal and there is money to be made from it.

In addition, cybersecurity remains deeply siloed. According to Vasco Gomes, Global CTO for Cyberproducts, Atos "it is typical for organizations to have somewhere between 15 and 50 different security technologies, and enough staff to be expert in about five of them, which does not help with the shortage of skills challenge."
So how do we square the level of threat and complexity with the huge shortfall in cybersecurity professionals and what can organizations do to protect themselves?

Start with education

There is a startling lack of vocational courses available that are dedicated to cybersecurity. Despite its complexity and necessity, it continues to form just a small part of a broader computer sciences curriculum. Industry is working to address this gap by partnering with schools and colleges to provide courses and information. Exposing students to the realities within the market and giving them the awareness of what's happening across the digital landscape is vital to improving knowledge. Cybersecurity is one of the most dynamic and changing areas in technology and a broad view is vital for learning.
Many governments are now also putting digital security awareness on the national curriculum to keep children and young people safe online. This early awareness may encourage more students to look deeper into the area.

Organizations themselves can also play a role in educating their employees on how they can help the cybersecurity effort and ensure it is viewed as a collective problem that needs to be managed. The main attack vectors are still around phishing and password security. Both can be managed down through a broad education program beginning at onboarding stage.
Explaining responsibilities and reporting principles are key. An active reporting line can be critical to an organization to identify attacks swiftly and mitigate their potential for harm.

Educate the C-suite

Nowhere is this more important than with the C-suite as executives are at increased risk of attack, particularly if they are well-known. They also need to understand the level of risk in order to set the right budget and priority for security across the business.

They must also consider the best way to manage security within their organization and avoid the temptation to keep the discipline entirely in-house. With experts in short supply, this can leave them exposed.

Partnership approach

A fully integrated partnership approach to security with the best tools, people and processes is the best approach.
When there is a shortage of professionals, we must pool our resources to support each other. Our professionals are continually learning and upskilling through wide access to data, labs and other professionals. We are able to hunt and detect threats proactively without being overwhelmed by the day-to-day volume of risks.

> When there's a shortage of professionals," says Catalina "we must pool our resources to support each other. Our professionals are continually learning and upskilling through wide access to data, labs and other professionals. We are able to hunt and detect threats proactively without being overwhelmed by the day-to-day volume of risks.

The digital landscape has changed beyond recognition over the last ten years and continues to accelerate. Technological breakthroughs in the 4.0 era have opened up possibilities in the way enterprises are producing, in the way we work and in the services offered to customers. However, they have also given rise to new security risks. Businesses are now highly distributed, broadening attack surfaces and giving rise to shadow IT. Data is stored and processed across numerous places – cloud, edge, and even swarms. Digital is moving into things with mass proliferation of IoT and the convergence of IT and OT.

With new risks come new regulations with legislative frameworks increasingly shaping the digital world as we know it: the General Data Protection Regulation (GDPR) and the Cybersecurity Act in Europe, and more recently in the US, regulatory changes to constrain the vital national services to a security approach after the Colonial Pipeline attack[7].

With boundaries increasingly blurred between physical and digital, the impact of digital security is no longer limited to business or legal but extends to environmental and human impacts. It must be seen as the vital ingredient in achieving operational resilience and supporting digital transformation. Within this context, CIOs and CISOs will have to tackle 5 main challenges in the years to come:

1 The "fortress" approach is no longer effective : boundaries between internal and external are blurring with front and center "*users*" (internal/partners/customers), "*assets*" (Bring Your Own Device - BYOD), "*data*" and "*applications*" which are cloudified, moved at the edge. This leads to a new resources centric, identity based paradigm and requires a segregated approach.

2 A transition will have to happen to move from a patchwork of IT / OT solutions and cyber solutions to modern architectures secured by design.

3 There is a need to guarantee a level of protection over time to face evolving threats complex architecture (multi cloud + OP, edge, etc.)

4 There is an increasing demand for setting up secure collaborative mechanisms in a world where the new normal will be common industrial data platforms[8], [9]multi-sided industry data platforms and digital models with ecosystem platforms.

5 Faster go to marker digital services and pressure on cost savings are leading to accelerated developments, (code resuse, Commercial Off-The-Shelf (COTS), etc.) There is a risk to vulnerabilities as organizations may not have the right expertise and security mechanisms in place.

Atos' take to address these challenges

- Organizations need to review their strategic business transformation plan, their state of legacy, their risks and transformation constraints to determine the best roadmap to strenghten their cybersecurity and transform their operational capacities. They should should set out an articulated approach and include a secure transition at business level.

- Risk assessment should be business-driven: everything is about choices. Organizations need to make tough security decisions (COTS building blocks versus customization, internalization versus external managed security services) based on based on the critical functions of their digital business. Organizations should evaluate the possibility for managed services to reduce complexity and guarantee that the level of time. It implies digital engineering as a first step.

- Data protection at the core: organizations can maintain the benefits of cloud use and cloud environments and ensure data protection with the right protective overlays (Bring Your Own Key, Bring Your Own Encryption).

- Implementing security-by-design approaches of the architecture, combining operational capabilities and security, will help reduce costs and improve efficiency. Organizations need to initiate groups bringing together expertise from IT, OT, and operations. Organizations should select in priority sovereign solutions or architectures and solutions compatible with technological innovations (post-quantum cryptography, biometrics, etc. will significantly boost productivity in the years to come).

In conclusion, Atos approach to digital security is based on two main **recommendations**:

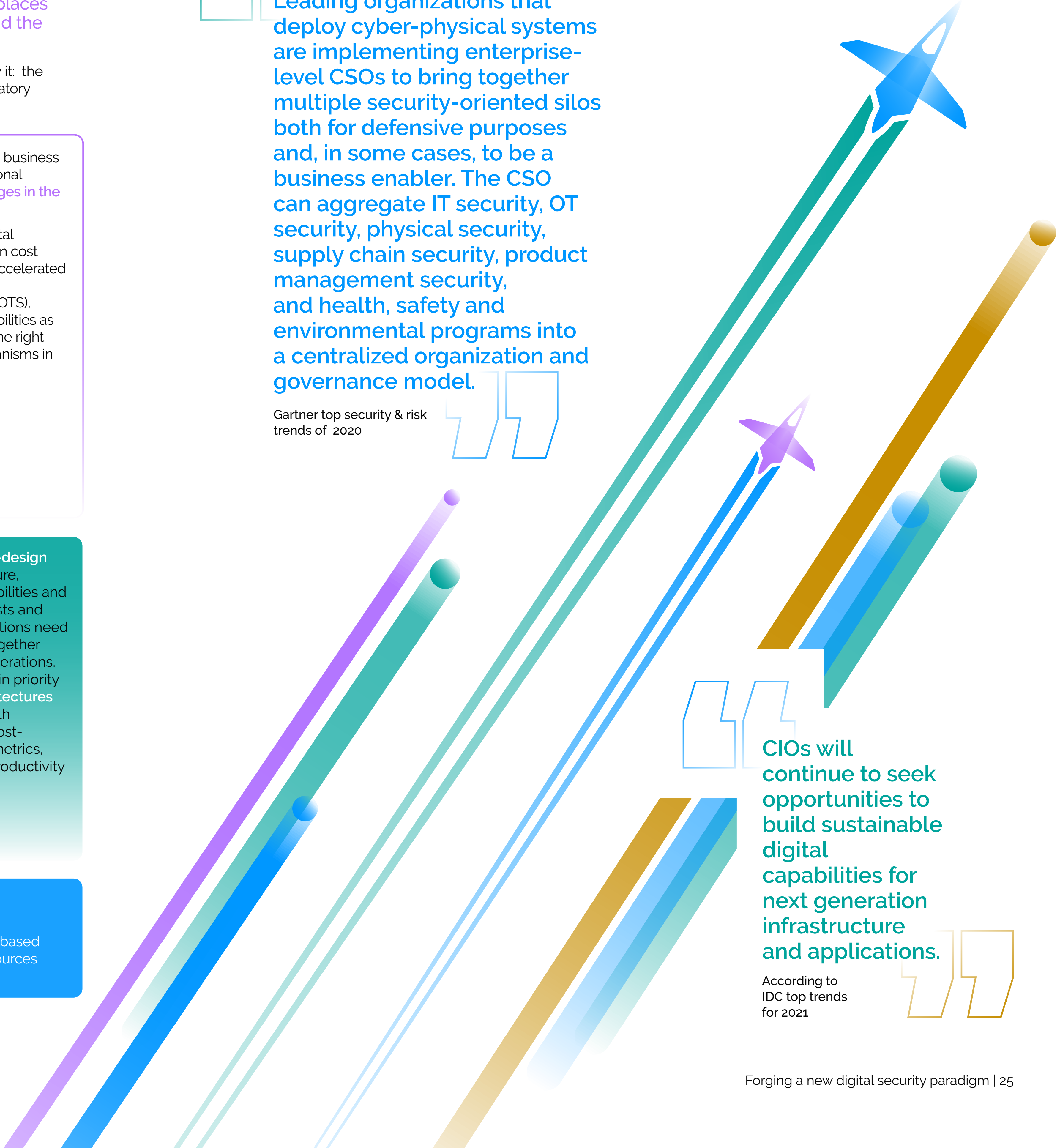
1 Develop a **corporate culture of security** across your organizations. Major efforts should be focused on breaking silos A transition is essential to move between operations and security.

2 **Adopt a zero trust approach**, based based on protecting your resources instead of your perimeter.

[7] lhttps://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

[8] Supply chain ecosystems established around Common Industrial data Platforms where participants will intentionally share data relating to design, production, operations and markets.

[9] Ex: "Consumer to grid", "Building to grid" and "Vehicle to grid"



> Leading organizations that deploy cyber-physical systems are implementing enterprise-level CSOs to bring together multiple security-oriented silos both for defensive purposes and, in some cases, to be a business enabler. The CSO can aggregate IT security, OT security, physical security, supply chain security, product management security, and health, safety and environmental programs into a centralized organization and governance model.

Gartner top security & risk trends of 2020

> CIOs will continue to seek opportunities to build sustainable digital capabilities for next generation infrastructure and applications.

According to IDC top trends for 2021

Digital security in manufacturing – coping with ransomware

By Vieri Tenuta, IT/OT and IoT Digital Security Offerings Manager, and Marc Llanes, Cybersecurity Global Business Development, Atos.

The challenge

The manufacturing industry is particularly vulnerable to ransomware attacks because their technologies and operating systems are often legacy and do not lend themselves to security patches or updates.

"Ransomware is often misunderstood," suggests Vieri Tenuta, IT/OT and IoT Digital Security Offerings Manager at Atos, "it's highly prolific, easily developed and operates well in a low-tech environment as it exploits vulnerabilities in legacy systems that have no in-built security and relies heavily on social engineering. Up until recently, manufacturers found a level of security through obscurity as their systems were isolated but now that they are increasingly connected, there is a real issue."

The risk

A malware attack can bring a manufacturer to a halt and prevent business from resuming. It is extremely hard to recover from an attack. In many cases the road to recovery – without any back-up in place – is almost impossible. You cannot break an encryption and often attackers can change encryption keys once an attack has been executed and re-attack.

Many organizations will pay the money immediately to recover. "I know manufacturers who have refused to pay, and their business has been disrupted, sometimes up to a year. It's an extremely hard road." says Tenuta.

The situation will be further complicated by new regulations surrounding cryptocurrencies. It is likely that the EU and US will look to ban crypto anonymity to prevent the funding of criminal activity through payment of ransoms. Although any movement to prevent ransomware is welcomed, further thought is required on practical support to organizations targeted rather than simply criminalizing organizations who feel they need to pay to resume operations.

Atos approach

Atos adopts an approach to security that covers people, processes, and solutions..

1 **People**: to reduce ransomware attacks requires all employees to understand what an attack might look like and to take steps to protect and alert against threats. This is a strong defense against ransomware.

2 **Processes:** a risk assessment and adequate data classification is required for an organization to understand how they would manage a ransomware attack. The cost / risk analysis of paying vs not paying must be played out and scenario planning for every eventuality should be in place.

3 **Solutions:** managed detection and response are needed. Utilizing tools and people, particularly AI, that can monitor user behavior and identify attacks before they take hold is vital.

Security-enabled transformation in financial services and insurance

By Ian Cole, Group Industry Director Financial Services and Insurance and Olga Portilla, Cybersecurity Products Offering Manager, Atos.

The challenge

Financial service and insurance organizations are on an accelerating journey toward digital transformation, ahead of most other industries, raising the demand for digital interaction and cloud migration. They also hold sensitive data for their customers and must ensure confidentiality and regulatory compliance with a raft of different regulations to adhere to such as PSD2, PCI-DSS.

They were the most-attacked industry for the fifth year running in 2020. Security, therefore, is fundamental to avoiding disruption to service, gaining and maintaining trust, protecting reputation and achieving a competitive edge.

The risk

The risks for financial institutions of getting their security wrong are enormous. A data breach can impact their credit rating and lead to a loss of trust from their customers who can easily take their business elsewhere.

Exposure to risk has also been exacerbated by the pace of change in digitization and the recent move to remote working during the pandemic.

Atos approach

Security and trust must be built into the broader business strategy, taking consideration of long-term goals, primary risks they face and the value-add they want to bring to customers.

Atos's strategy is based on three strands:

1 Understand what the business is trying to achieve – their digital transformation and business strategy and the critical risks they need to address.

2 What does this strategy mean for the technology, people and processes and the security principles that need to be addressed as part of development?

3 How do we translate the above into delivery using an agile methodology with risks and regulations considered as part of security by design upfront?

This approach is also supported by a range of security products, including Trustway encryption solutions, IDnomic for trusted digital identities and Evidian Identity and Access Management solutions.

> We now build with a Zero Trust approach to security. We establish security boundaries through identity least priviledge credentials and access management, enforcing the security policy and trust domains at an architectural as well as a technical level."
>
> **Ian Cole**
> Group Industry Director Financial Services and Insurance,
> **Atos**

Digital security of healthcare in the advancement of IoT

By Marjolaine Lombard, Cybersecurity Products Offering Manager, Atos.

The challenge

According to Frost & Sullivan's Internet of Medical Things (IoMT) Forecast to 2021 report, 20 billion to 30 billion connected IoT and medical devices are part of the healthcare ecosystem. This presents a substantial additional threat to the healthcare sector, which will impact healthcare providers, pharmaceutical companies, manufacturers, and patients. It will also require adherence to regulation and legislation that covers the management, security, and privacy of data.

The benefits of wearables within the healthcare sector are huge but they are easily exploited in lateral attacks and ransomware.

The issue of data management and security is extremely complex within the healthcare sector with questions around who owns the data, processes the data and is ultimately responsible for its security.

The risk

Put bluntly, there is a risk to life if wearables and medical devices are not secure. The integrity of the data they hold is vital for patient care and any compromise in the use of devices such as pacemakers could have devastating consequences. This risk is also present across life sciences, if medicine or vaccine production data is compromised.

Atos approach

Data needs to be encrypted in transit and at rest and through each stage of a process. It helps us guarantee that only those with the right authentication can access sensitive data. On top of this, we use key management solutions, identity management, biometric identification solutions and electronic certificates to manage networks and gateways. This means data remains confidential and ensures a person's right to privacy.

Blockchain is also emerging as a useful tool in data governance and ensuring the chain of responsibility is managed, monitored and verified.

Atos is also using biometric identification for a pharmaceutical manufacturer ensuring the secure log-in of employees on the production line through the wearing of an innovative wrist band. Beyond security, the solution has increased efficiency, transparency and productivity.

> Encryption is an extremely powerful tool for data security within healthcare.
>
> **Marjolaine Lombard**
> Cybersecurity Products Offering Manager,
> **Atos**

Securing the digital future of public transport

By Barbara Couée, Portfolio Manager in Digital Security, Atos.

The challenge

Public transport systems form part of critical infrastructure, moving people and goods across the country every day. For this reason, they require the systems in place for security to be managed as a priority. This also means that they are subject to strict regulation and normative standards that must be complied with.

Connected and autonomous transport systems need to combine safety and security on board and on the ground:

- Networks and systems on board (primary systems as well as CCTV, intercom),
- Train-to-ground communications,
- Central administration systems on the ground.

Also, the interfaces with external systems such as police stations require high levels of performance and interactions, while in the meantime segmentation, protection and – more than ever – resiliency are required to ensure a high level of security - and at the end of the day, preserve passenger safety.

The risk

Connectivity will have to reach high performance in order to transfer massive flows of data and manage operations in real time, whether it is for operational systems maintenance or cybersecurity. So much data will be produced, it will need to be stored, managed and pre-processed onboard and at the edge.

Atos approach

"The conversations we had previously with rail operators were oriented on our expertise in embedded products, critical communications and integration. The new era is oriented around digital capabilities such as embedded computer vision, edge computing embedding AI closer to the sensor, and cybersecurity to manage railway specific risks."

This will enable the innovation of tomorrow related to 5G/LTE, AI and edge with the right level of cybersecurity.

Combining deep expertise in railway normative standards and state-of-the-art cybersecurity expertise are vital. Only with these two teams are we able at Atos to offer clients a powerful holistic approach in the secure digital transformation of public transportation.

What new security measures to embrace the 5G revolution ?

By Barbara Couée, Portfolio Manager in Digital Security, Atos.

The challenge

The promise of 5G is to develop and enhance new business models and possibilities for all markets and deliver the full potential of innovative technologies. Use cases such as smart cities, autonomous cars, remote surgeries, real-time remote-controlled operations and AR/VR in critical environments will require flawless IIOT-OT and 5G security to avoid human, environmental and economic damage.

With such a promise, private mobile networks are a major trend. IDC estimate that by 2025 75% of enterprises in industrial verticals like manufacturing or logistics will adopt private 5G networks.

With 5G private networks, and the associated slicing capabilities, enterprises or organizations will gain agility and efficiency in the allocation of resources by managing quality and consistency of service according to need and sensitivity. The technological breakthrough behind 5G (VNF/NFV, SD-Networks) will change the offering landscape and enable enterprise to implement their own 5G networks with low CAPEX /adjustable OPEX, while the expected benefits are significant.

At a wider scale, there are also clear benefits for public networks. Cities, such as New York and London, are planning to begin initiatives for building connectivity infrastructures for public utility and Smart Cities use cases by federating an ecosystem of telco, vendors, and digital players, providing buildings blocks and platforms to manage security and operations at the scale.

The risk

However, according to OMDIA survey completed in 2020, one of the issues that is still preventing enterprises from deploying 5G networks is integration with legacy systems (42%), while "reliability and quality of service" are the main perceived advantages (45%).

As there are many technology options, providers, deployment models, we see questions around:

- **How to choose?**
- **How to integrate with legacy systems?**
- **How to secure?**

Enterprises will have to navigate a large landscape of offerings mixing telecommunication operators , cloud service providers, cloud communication service providers and cloud-computing giants. They will have to choose the best business and operating model for their needs while ensuring networks are secure.

"5G will not only herald a new technological era but will also require major updates in the security approach, as new vulnerabilities will overlay traditional threats", says Barbara Couée, Portfolio Manager in Digital Security, Atos.

Atos approach

Enterprises will need a trusted 5G security orchestrator to implement a holistic 5G security program, mixing organization, processes, services, interconnections, data, protocols, network products, and orchestration to secure the new virtualization infrastructure, the software defined network, and the new network functions.

When building a 5G network, organizations need to identify the risks, classify their data, develop the end-to-end security strategy and define the threat mitigation plan.

To deploy a 5G secure-by-design network, essential security questions must be addressed such as:

- What data will need to sit where and therefore what security levels will be required?
- Which services are critical for your operations/business and must always be protected?
- What are the security controls that must be implemented (APIs, containers security, SDN, NFV)?
- How can we detect and respond effectively and efficiently to cyberthreats

Securing collaborative combat

By Valérie Petat, Business Unit Director, Air, Land and Sea electronics/ Industrial services and solutions and Norbert Di Costanzo, Chief Operating Officer and senior member of the Scientific Community, Atos.

The challenge

Ten years ago, cyberthreats and cyber warfare were not on the defense sectors' radar. This means that legacy hardware and software across fleets of vehicles for air, land and sea need updating and securing for a new digital world. But just as heavy armour can be counterproductive on the battlefield, digital security defenses can hinder systems operations: a balancing act is needed.

While this upgrade is ongoing, threats are on the increase and constantly evolving with a need for manufacture and design of systems to be future-proofed and adaptable to an ever-changing threat environment, requiring constant risk assessment and maintenanceAn additional hardware challenge is that major constraints in terms of weight, size criteria and power consumption have to be taken into account.

The risk

As defense moves into a new era, collaborative combat is vital in managing security situations. The ability to securely pass information from different locations in air, on sea and on land will become a necessity. Unless the integrity of information can be guaranteed, there is significant tactical risk to operations.

Any interception, tampering or lack of availability of tactical information could be devasting to a mission and would have a direct impact on its success or failure.

Atos approach

Atos has developed a new generation of combat aircraft's multi-level gateway system, enabling secure two-way transfer between networks with different levels of security and confidentiality, thus preserving data integrity and security of all onboard connectivity. It allows critical "*authorized*" intelligence to be safely shared and used at all times, protected against outside intrusion.

Atos has security embedded and by-design with dedicated cybersecurity experts forming part of every project team ensuring the required standards are met and that the design is future-proofed for necessary security updates as threats and technology evolves. Each component of both the hardware and software is vetted for security and we rigorously laboratory test each part.

The system itself is tamper-proof and only a small and highly trained team within our organization can work on these solutions that are designed and delivered in-house only and meet strict French security criteria.

Digital security: what does the future hold?

By Zeina Zakhour, Global CTO for Digital Security, Atos

The digital revolution holds the promise of great change for good. As our population grows, a connected digital society could bring further equality and has the scope to improve people's lives. However, this must be underpinned by digital security, a concept that encompasses privacy, ethics, cybersecurity and public safety.

The only constant in digital is change. Within a few decades, digital will be everywhere, including in our physical lives and even, perhaps, augmenting our bodies.
Over the next years we will see networks changing with the advancement of 5G and possible introduction of 6G, the further convergence of physical and digital worlds and the management of data moving from the center to the edge, in swarms or within devices and things. However, these advancements will fail unless they can be secured.
Digital cannot function without security. The risks are too great, and advancements will slow down or cease.

The need for ambidextrous cybersecurity innovation

The ever-growing and complex surface perimeter of organizations requires a new holistic approach to security. Simply put, if security is not embedded, it will fail. Building a fortress to protect doesn't work in these distributed settings where data is pervasive, and the new single point of failures are the APIs. Therefore, the new security perimeter must be built on identity – controlling the digital identities and permissions of all the people, applications, and machines in your environment.
All those fundamental changes will require an ambidextrous cybersecurity innovation process, focusing both on incremental and disruptive innovations. We, at Atos, work on incremental innovations improving existing cybersecurity technologies to bring visibility, simplicity, agility, and efficiency to our security operations.
While in parallel we create disruptive cybersecurity innovations that will transform how we consume and provide security.
It means investing in AI for digital security not only for advanced detection and response but also shifting left to the protection controls addressing compliance and gaps before the cybercriminals discover them, and leveraging AI in public safety solutions to enhance and empower first-responders. As another example, Atos Cryptography R&D is focused on privacy-preserving cryptography such as homomorphic encryption to maintain data encrypted throughout its lifecycle, or even preparing for post-quantum cryptography.

Regulation, legislation, and control

A key element in the future of digital security is around regulation and legislation. Standards and frameworks are being developed for emerging technologies and networks such as AI, 5G, edge, IoT and OT.
Hard lessons have had to be learnt from past mistakes in (not) securing IoT and cloud environments. Now and in the future, there will be greater emphasis on private and public sector working together to share knowledge and develop frameworks and regulations that maintain a safe and secure digital space. Atos already works with industry players and with the European Union in this space through initiatives such as the Charter of Trust and the European Cyber Security Organization (ECSO). This will expand to become more global in remit and to cover issues such as ethics and trust in emerging technologies.

The role of privacy and ethics

In the future, digital security will expand to encompass the prevention of harm. It will be vital in maintaining the integrity of data and transparency of algorithms in artificial intelligence and machine learning.
You cannot decouple the issues of security with privacy and ethics. They are interdependent and will become the foundation from which we build our digital revolution moving forwards. Auditable and transparent data management will enable the future digital world, as long as its integrity is guaranteed by security.

Acknowledgements

We would like to thank the following contributors. If you wish to send feedback, please tweet using #WinningTheCyberRace or contact us

Cyril Dujardin	SEVP, Head of Digital Security
Lukasz Olszewski	Former Global Head of CERT
Maciej Zarski	Global Head of CERT
Eyal Asila	Head of Digital Cyber Consulting
Vasco Gomes	Global Chief Technology Officer for Cybersecurity Products
François Cortial	Chief Technology Officer, Mission-Critical Systems
Eric Wahed	Global Head of Public Safety / NG112
Paul Bayle	Head of Security and CSO
Vinod Vasudevan	Global CTO MDR
Deborah Dillon	Head of Protection and Privacy
Catalina Dodu	Global Presales Director for Cybersecurity Services
Vieri Tenuta	IT/OT & IoT Digital Security Offerings Manager
Marc Llanes	Cybersecurity Global Business Development
Ian Cole	Group Industry Director Financial Services and Insurance
Olga Portilla	Cybersecurity Products Offering Manager
Marjolaine Lombard	Cybersecurity Products Offering Manager
Barbara Couée	Portfolio Manager in Digital Security
Valérie Petat	Business Unit Director, Air, Land and Sea electronics/ Industrial services & solutions
Norbert Di Costanzo	Chief Operating Officer and senior member of the Scientific Community
Zeina Zakhour	Global CTO for Digital Security

About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of over € 11 billion.

European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos operates under the brands Atos and Atos|Syntel. Atos is a SE (Societas Europaea), listed on the CAC40 Paris stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together