Cybersecurity Trends

UK edition n.2 / 2022

The Cloud and it's evolution: Why settle for one?

BLOCKAPT™

Resilience - Cybersecurity & Business Risks...

BLOCKAPT™

A centrally managed **COMMAND** & **CONTROL**
single platform experience.

Eliminate the weakest link.

info@blockapt.com

blockapt.com

Contents

Editorial

Murky times for murky affairs... RESILIENCE is paramount.



Authors: Raj Meghani, Marco Essomba, Laurent Chrzanovski

With raw material prices skyrocketing and stock exchanges in a panic as a consequence of the Ukraine/Russia war, while the pandemic is not yet vanquished, we are probably living in one of the most dangerous business years since 1929.

In these conditions and since 2020, it is open season for global players to buy or endanger concurrent companies, and the current cyber-risk level is way higher than that during the records reached during the lockdown periods.

In addition, attacks are generally hitting companies which are already struggling to survive or to relaunch their activities after two years of struggling to stay afloat amongst this deep crisis.

In this context, after years of focusing on providing very strong data protection to organisations and institutions, because of the implementation of the GDPR and of the Cloud Act, it is a must to protect the "crown jewels" of any business.

In this latest issue of Cybersecurity Trends UK, we focus on resilience within risk and cloud management. Informative articles enable you to better understand the cyber-risks in all their forms, as well as tools and measures to take swift countermeasures in order to mitigate them.

Hybrid or multi-cloud is a hot topic and one of those measures. It allows, without too much effort, to swiftly apply a new segmentation to your data and your "crown jewels", implement new access credential rules, overcome 'Lock-in' and exit the solution of having "all your eggs in one single basket". No longer is there a requirement to settle for one cloud when you can have the opportunity to flex your business operating model within a true hybrid cloud environment.

A new way of flexible working helps business growth and scalability, reduces the dependence on one cloud supplier and their pricing models and puts the business back in control of how and where they want to manage and secure their data across the world, subject to different judicial restrictions.

We also focus on the risks associated with both business and industrial espionage. Awareness on this topic is poor at best in too many countries. Others such as the Swiss Confederation, along with the USA and Israel, have already led the way through targeted campaigns which alert businesses on the "highest risk possible".

During what appears to be the year when "the sum of all fears", on earth and in the digital space, are converting into dramatic realities under our eyes, day after day, we hope this thought-provoking issue will bring you some useful and clearly explained concepts to help beef up your business security at home, at your office or in your cloud environment. ■

Hybrid multi-cloud: what challenges lie ahead?

Author: Federica Maria Rita Livelli

Scenario

The adoption of flexible working arrangements has literally exploded with the healthcare emergency over the last two years and, at the same time, the cloud has become a key driver of business growth, helping to accelerate the implementation of new technologies to improve performance and speed up the ongoing process of digitisation and innovation.

In particular, the hybrid cloud market is growing and, according to research firm *Mordor Intelligence*, is set to grow at an average annual growth rate (CAGR) of 21.06% from 2022-2026. In addition, there is also a growing trend towards hybrid multi-cloud solutions, as confirmed by the recent *Enterprise Cloud Index (ECI)* study: 36% of enterprises surveyed globally are already using hybrid multi-cloud solutions, and it is estimated that this figure could rise to 64% in the next 1-3 years.

The use of hybrid multi-cloud platforms is a key tool for ensuring access to resources and services essential for remote and mobile working, and the

significant growth of the hybrid multi-cloud market compared to other cloud services is driven by the fact that it offers certain advantages required by organisations with huge data sets and processing needs.

In fact, using a hybrid multi-cloud allows companies to scale their computing resources and eliminate the need to invest huge capital to handle short-term peaks in demand, even in cases where the company needs to free up local resources for more sensitive data or applications.

Hybrid multi-cloud: how to approach it

It is worth mentioning that the hybrid multi-cloud environment eliminates the use of a single cloud, providing the use of two or more public clouds

and even private clouds and becoming a strategic lever to ensure business processes and business rules are extremely 'agile' and *'adaptive'.*

In fact, with hybrid multi-cloud, organisations can move workloads anywhere (i.e., public cloud, on-premises data centre or edge) as well as giving IT the flexibility to accelerate the organisation's digital transformation.

In addition, in terms of privacy and security, highly regulated organisations can successfully use hybrid multi-cloud to store sensitive information on-premises, while less sensitive workloads are transferred to the cloud, ensuring better performance and cost savings.

In addition, a hybrid multi-cloud strategy ensures:

- non-dependence on a single supplier
- greater flexibility and scalability
- greater granular control needed to comply with complex laws that can vary widely between national and regional jurisdictions.

However, technology alone is not enough, and it is essential for corporate IT teams to take a thoughtful, strategic and detailed approach to ensure a successful and efficient implementation of hybrid multi-cloud through:

- analysis of the internal and external context in which the organisation operates in order to obtain a census of hardware and software products;
- identification of potential risks in the face of the ever-increasing scenario of cyber attacks and ongoing cyberwar;
- measuring the impacts of the identified risks; implementation of measures to minimise its attack surface;
- the implementation of a comprehensive organisational security policy. In this way, the organisation is able to embark on a path of knowledge of the interconnections between business and information systems.

Risk Management, Business continuity & Cybersecurity vs. Hybrid multi-cloud

It is worth mentioning that organisations can benefit enormously from implementing the principles of Risk Management, Business Continuity Management and Cyber security Management as they move towards

hybrid multi-cloud adoption. These disciplines, in fact, become strategic levers and support organisations in the adoption of multi-cloud hybrids:

- the design and implementation of the hybrid multi-cloud strategy from a *risk-based* and *resilience-based* perspective;
- the completion of the accelerated process of digitisation and innovation underway;
- a clear vision of corporate governance and compliance;
- compliance with the regulatory and contractual requirements of the market in which the organisation operates.

Moreover, organisations - always from a *risk-based* and *resilience-based* perspective and in terms of the cloud provider selection process - must also verify the implementation by the cloud provider of the principles of Risk Management, Business Continuity and Cybersecurity, which must be able to:

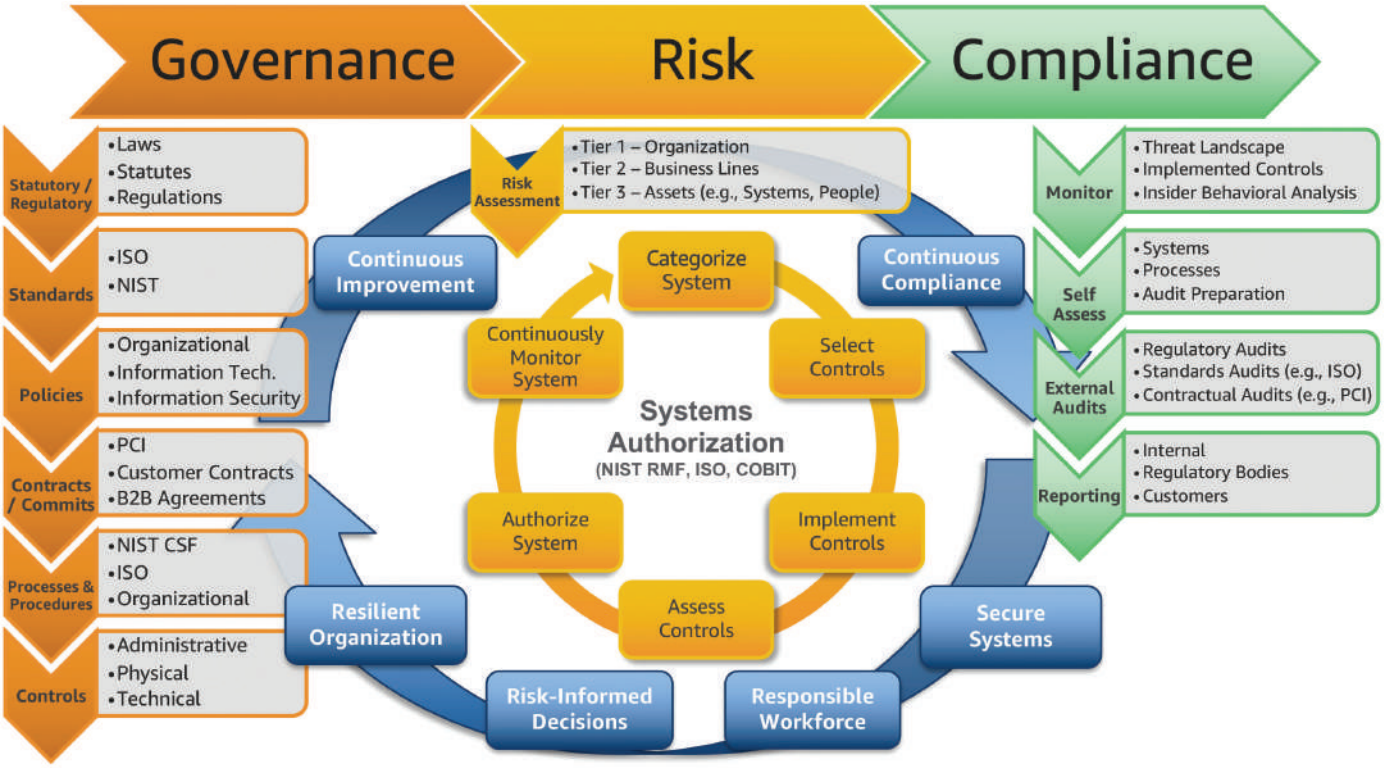
- demonstrate the existence of both their own and subcontractors' continuity plans;
- provide the specifications of the data centre used;
- ensuring connectivity services and power supply in data centres in case of disaster/disruption;
- manage hardware failures efficiently (it is desirable to contractually include the way in which they are resolved);
- ensure a report in terms of scheduling recovery and emergency tests;
- ensure the authenticity, confidentiality, integrity and availability of data.

Hybrid multi-cloud security

In an increasingly uncertain cybersecurity landscape, it is crucial not to rely entirely on hybrid multi-cloud for security, as although tools such as two-factor authentication, encryption and automated alerts can help

BIO

Holder of Business Continuity certification - AMBCI BCI, UK and CBCP DRI, USA, Risk Management FERMA Rimap®, Business Continuity & Risk Management consultant, Federica Maria Rita Livelli carries out dissemination and development of resilience culture at various institutions and universities.
She is a member of: ANRA Board; Board of the BCI Italy Chapter; Scientific Committee of CLUSIT; Women for Cyber Security (Technical Committee); various UNI technical committees . She teaches introduction modules of: ISO 22301 - Business Continuity & Resilience (POLIMI-BOCCONI University and University of Verona, University of Cagliari, Environmental Master University of Padua, University of Castellanza LIUC) ; ISO 31000 - Risk Management (State University of Milan and University of Castellanza, LIUC); speaker and moderator in several seminars, national and international conferences. Author of numerous articles in several online journals as well as having participated as co-author in: 2019, 2020, 2021 and 2022 editions of the Clusit Report - Cyber Security; CLUSIT thematic books ref. Artificial Intelligence (2020) and Cyber Risk (2021); Book "Lo Stato in Crisi" (2021) ed. Angeli.



protect networks, in reality no network is inviolable, especially if no additional security measures have been applied. Therefore, a good hybrid multi-cloud security strategy should include ensuring:

- correct configuration;
- an update of hardware and software system patches;
- backup data storage and offline archiving.

Organisations will then be able to address the key challenges that hybrid multi-cloud adoption brings in terms of security, compliance, trust, performance issues and, where necessary, implement a policy transformation strategy to ensure:

- better governance;
- increased compliance;
- increased corporate value;
- increased operational efficiency and privacy;
- mitigation of security risks;
- increased digital and data visibility.

By doing so, it will be possible to implement a holistic approach to ensure constant visibility across endpoints, networks and even multiple cloud environments. In addition, adopting a zero-trust approach and introducing more automation supported by AI and ML can further help to keep the hybrid multi-cloud secure, not to mention that it is also important to have qualified and continuously updated IT staff.

We recall that, especially when it comes to critical infrastructures, the continuity of supply of public utility services has top priority and must be maintained, to ensure that no damage occurs to people, the environment or process systems. Therefore, security must be increasingly widespread, updated and structured according to solid, validated and shared criteria.

Shadows on the holistic horizon

The adoption of hybrid multi-cloud, while a game-changer for organisations, is not without its shadows. Indeed, while hybrid multi-cloud provides organisations with the scalability and flexibility to remain competitive and innovative in an ever-changing global landscape, it also brings with it the management of new security risks and makes it increasingly necessary to safeguard corporate data in the face of a variety of factors.

Conclusions

As cybersecurity issues continue to proliferate, organisations see the adoption of resilient and flexible IT solutions as a fundamental requirement. As a result, the implementation of hybrid multi-cloud is the most natural path to holistically manage risk, business continuity and cybersecurity in the organisation. However, given the shadows we have just mentioned, the organisation, in order to ensure its organisational and operational resilience, will have to implement cloud cybersecurity standards, Risk Management and Business Continuity principles, as well as incorporate the recommendations and adopt the checklists made available by international bodies such as the *Cloud Security Alliance (CSA)* that clarify best practices and provide guidelines on how to manage the various types of clouds and the risks they entail. ■

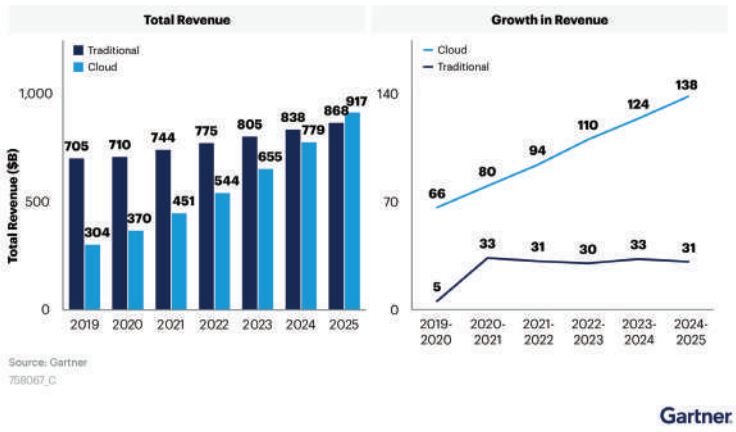
The Cloud is a business enabler, yet complex.

Author: Nicola Sotira

Whether it's working from home, or from the much-loved distance learning up to financial transactions and business processes, the Cloud and its related technologies are at the heart of this digital transformation and new business models.

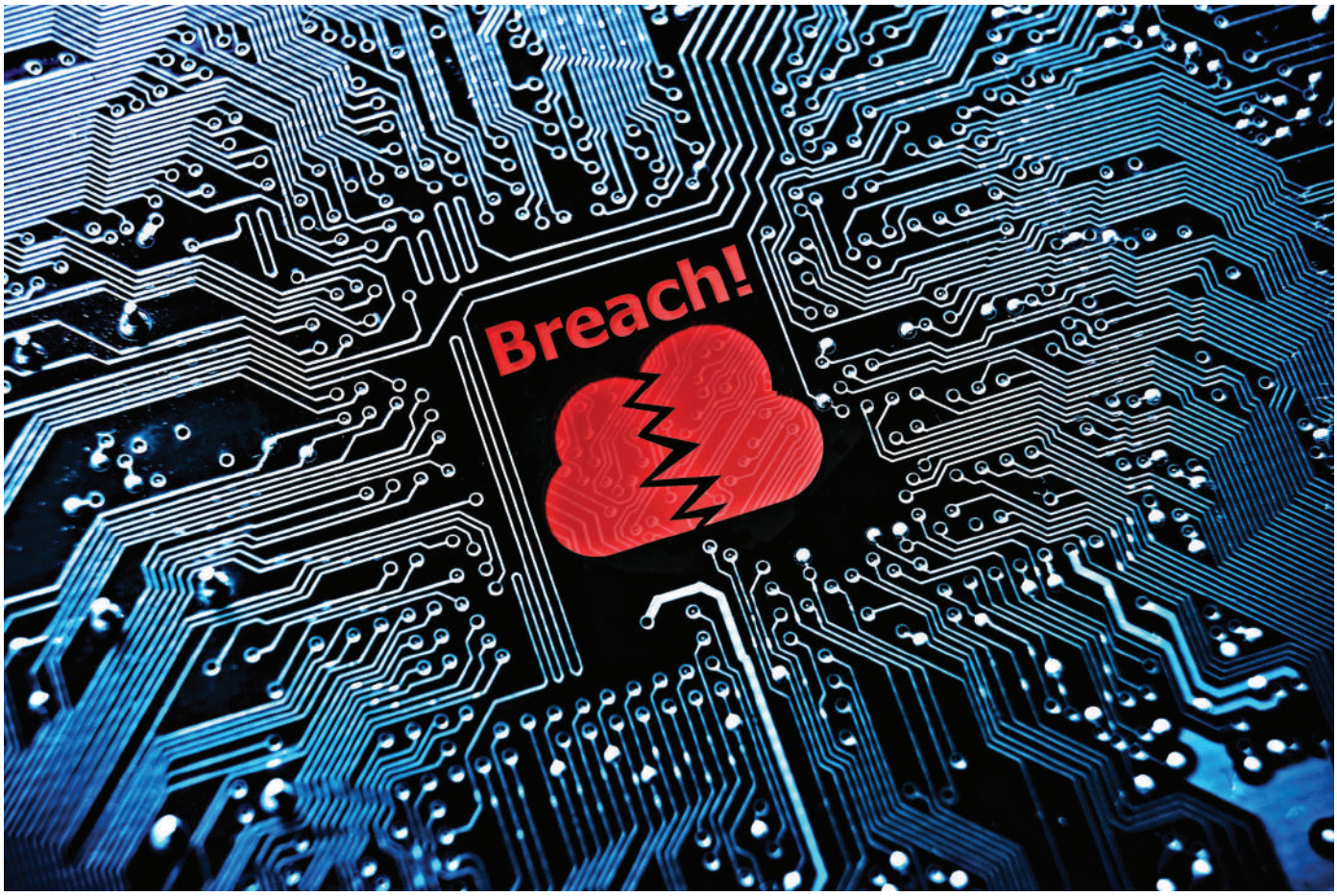
One can safely venture to write that the Cloud is a business enabler. The pandemic accelerated the digital transformation journey and even now, as organisations are slowly returning to pre-Covid levels, the Cloud continues to remain a relevant tool for accelerating digital transformation plans by offering smart, accessible and agile digital solutions.

With the use of Cloud technologies, many of the barriers to entry for digital transformation are reduced, facilitating the implementation of new digital processes even in industries that typically have little to do with technology and can instead reap the benefits of modern IT solutions and infrastructure. Today, the Cloud enables high scalability, storage capacity, simplified access and is in line with new mobile technologies. Obviously, when it comes to the Cloud, the issue of security also becomes relevant and service providers are investing a lot in this area and, on average, are protecting their infrastructure very well.



BIO

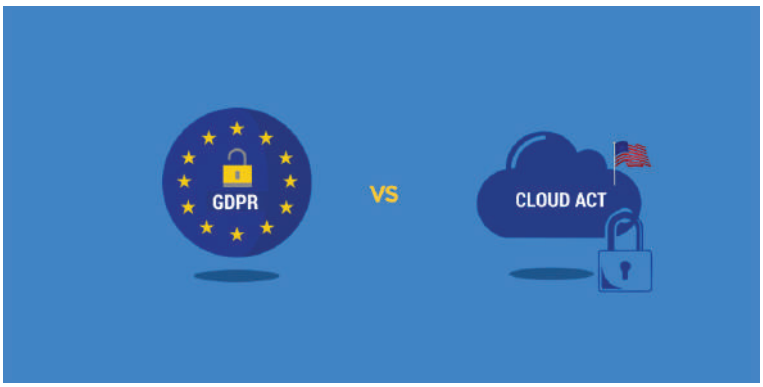
Nicola is Head of CERT in Poste Italiane . He has been working in information security and network for more than twenty years, with vast experience gained in international environments. He was involved in encryption design and network security in the security area, also working in complex infrastructures like mobile and 3G networks. He has collaborated with several magazines in the computer industry as a journalist contributing to disseminating issues related to Security and legal, technical aspects. Since 2005, he's been teaching on Master in Network Security of the Sapienza University. Member of the Association for Computing Machinery (ACM) since 2004 and promoter of technological innovation, Nicola collaborates with several start-ups in Italy and abroad. Member of Startup Italy since 2014, where he helped companies in their development and design of services in the mobile sector; Nicola collaborates with Oracle Security Council since 2014. He is also General Director of the Global Cyber Security Foundation (GCSEC) from 2016 and member of the CERTFIN (Italy's Financial CSIRT).



According to research by Gartner, many of the breaches we see today in this domain are configuration and posture errors attributable to the customer. Cloud services require a shared design approach between the Cloud operator and the customer to be successful.

Finding the right balance between security and innovation is not easy and often turns into a kind of complex puzzle to solve for all those organisations venturing into a driven process of transformation. The only way to solve the puzzle is to integrate the transformation teams with the cybersecurity teams by building a journey in which the security strategy is present from the start. The right balance requires a robust cybersecurity strategy that is absolutely aligned with digital transformation and business objectives. A security that must be involved in the various project streams. Compliance and legislative issues must also be included in all these considerations.

Another issue that is being discussed again is the Cloud Act (American federal law of 2018), which allows secret services and law enforcement agencies to access all data stored by American companies even if they are located outside the territory of the United States. A rule that clashes with the provisions of the GDPR, just to mention one of the actors. The United States and the European Union are again returning to the subject, with the Americans declaring their commitment to ensuring that monitoring activities are proportionate to national security objectives.



In short, there are several open games on the subject that make us realise that living in the clouds will require a certain amount of effort. ■

The power of clouds – why settle for one?

Author: Raj Meghani

The inception of the modern-day cloud was launched almost 2 decades ago.

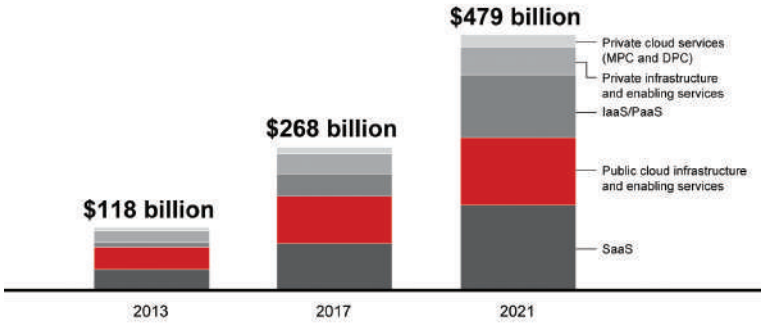
3 years ago, I spoke with a well renowned contact and asked him what the top barriers to cloud adoption were. Security was the common denominator – data security and general security risks.

BIO

Raj Meghani is Co-Founder & Chief Marketing Officer at BlockAPT. A leading edge, highly acclaimed, UK based innovative cybersecurity business, empowering organisations with a centrally managed, command and control single platform experience.Raj has also been appointed as a Non-Executive Director to the Board of Money Matters Bank. Passionate about turning the complex into something simple in cybersecurity, technology and digital transformation, Raj has over 25 years' experience in FTSE100/250 to high growth ventures helping businesses across financial services, IT and professional services with their business strategy, digital transformation, growth and retention plans. Raj is Editor for Cybersecurity Trends UK which has a global presence and is active in thought leadership and knowledge transfer of cybersecurity and business risk management.
LinkedIn - https://www.linkedin.com/in/raj-meghani-a036482/
Twitter: https://twitter.com/blockapt
Company website: https://www.blockapt.com

Fast forward to today. The COVID-19 pandemic with its remote workforce still has devastating ramifications for businesses across different vertical sectors, the Ukraine/Russia crisis has amplified cyber and nation state attacks, businesses of all sizes have opened their eyes as they remain on high-risk alert and are looking for more scalable, flexible, cost-effective solutions. The shift to the cloud has been one of the measures that have seen a rapid increase.

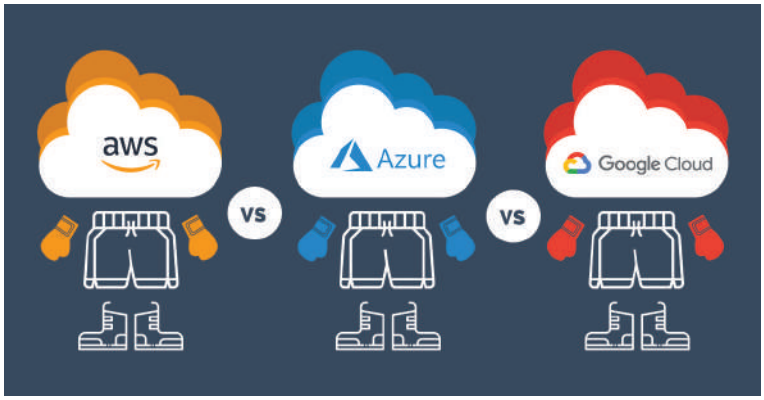
Global cloud IT market revenue



Notes: IaaS is infrastructure-as-a-service; PaaS is platform-as-a-service; SaaS is software-as-a-service; MPC is managed private cloud; DPC is digital private cloud
Sources: International Data Corporation (IDC); Gartner; Forrester; industry participant interviews; Bain & Company

Gartner predicts that by 2025, 51% of IT spending (within the application software, infrastructure software, business process services and system infrastructure markets) will have shifted from traditional solutions to the public cloud compared to 41% in 2022.

The numbers are staggering and the opportunities for providers such as Microsoft Azure, Amazon Web Services (AWS) and Google Cloud are on



an upwards trend as cloud technology gets assimilated into business infrastructure and becomes their modus operandi.

So why are so many organisations still struggling to overcome some of the barriers? What are they and how can some of these myths be debunked?

I have already invested in my own data centres and my security is sufficient.

Whether your infrastructure is on premise or on the cloud or a mixture of the two, many organisations fail to detect and identify the source of the increasing number of cyberattacks. Having sufficient security controls is paramount to ensure scalability and business continuity.

Cloud service providers have invested billions in ensuring they have the right cybersecurity methodologies and tools to enhance security for their customers and continue to do so. Although, on premise applications may be secure, reliable and allow businesses to maintain a certain level of control, the sheer effort and cost of managing and maintaining hardware, software licenses, integration capabilities, incident response management not to mention keeping hold of skilled staff and training increases the organisation's risk exposure and could be a barrier itself on the scalability front.

Moving to the cloud will automatically save me money.

Not always the case. It's a fairly simple concept as you only pay for what you use on the cloud. No sunken costs on hardware or replenishment, power usage, space, etc.

For example, In the case of a server, once you've reached the storage space limit, you are faced with purchasing a new server to increase bandwidth. Businesses with a seasonal trend on customer flows with an on-premise solution may not find it as cost-effective when traffic flows resume to normal levels and their server sits there with a high under utilisation rate.

According to the IDC, the most prominent industries who will be spending the most on cloud computing are those which deal with the most data yield – i.e., retrieving vast amounts of sensitive information from several different locations are Manufacturing ($20 billion), Professional Services ($18 billion) and Banking ($16 billion).

But caveat emptor - the cloud offers a long list of services, tools and options all of which can escalate costs for a business quickly if it is unprepared on its requirements. Most of them offer tools to help manage billing and costs but the onus is on the organisation to get the cloud optimised to meet their specific requirements in the first place.

If it ain't broke, then don't fix it right?

Wrong - unless there are strict regulatory, legal constraints on managing data. On premise, tried and tested legacy systems, applications, hardware, etc are not as agile as a cloud solution. If your business is looking to grow, scale up then the need to ensure your IT infrastructure can scale too is key. Add to this attractive cost savings and increased security levels wrapped into the service and it's only a matter of time before a digital transformation starts to show results.

Having my data on premise is safer than having it on the cloud.

Hmm. With only 1 in 10 organisations' apparently being able to analyse over 75% of their security events both on premise and in the cloud, the concerns around cloud security, data loss and data privacy still remain a big challenge for businesses of all sizes.

SMEs are not just looking to survive in these challenging times but save as much money as possible without compromising the security of their customer data. Often lacking in the relevant security expertise and knowledge, 40% of them have found it more cost-effective to employ third-party cloud platforms than maintaining an in-house system.

Of all the cloud services, studies show that management tools and security services are expected to be the fastest-growing segments with a 28.4% improvement.

With the traditional on premise set up, the onus is on the business to mitigate against cyberthreats. Staying on top of patches, security certificates, etc can often be missed. Cloud providers with their deep pockets are seen

to be on top of their game with security policies, compliance adherence, etc. In most cases, more so than what the traditional organisation has in place. Automation plays a key role here – intelligent collaboration and integration with change control processes across different devices, firewalls with robust threat intelligence, vulnerability management and incident response capability all boost the security ecosystem.

Interestingly, most public cloud breaches have been driven by an enterprise customer's insecure configurations. Gartner predicts that through 2025, 99% of cloud security failures will be the customer's fault NOT the security providers.

No business is guaranteed against cyberattacks – whether on cloud or on premise they are facing the same threats and risk exposure. The difference here is to do with responsibility and accountability.

Migrating to a cloud environment is going to be painful and disruptive.

Not always the case as it depends on the current state of a company's infrastructure. The business in the main has complete control over its software, policies and data. The flexibility to scale up or down on cloud usage is cost effective and provides economies of scale.

Treat the cloud migration as any other digital transformation project – with careful planning, a clear cloud strategy and implementation plan. Deployment compared to an on-premise solution is often quicker and less disruptive to the business. The key is in the planning. Plan. Plan. And plan again.

All my data is on one cloud so I'm tied in and can't use another one, right?

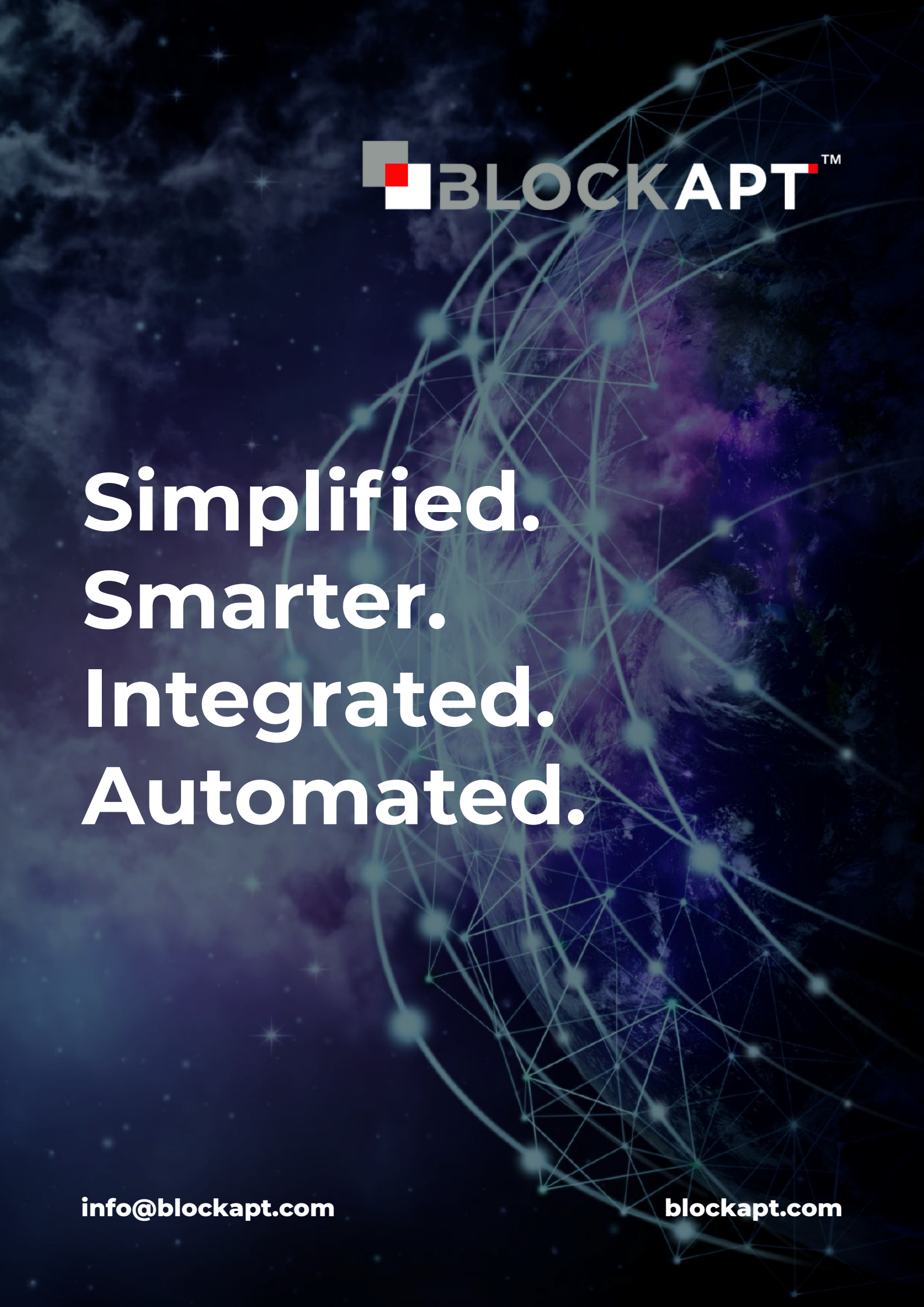
No. You can adapt your public clouds such as Microsoft Azure, Amazon Web Services (AWS), G- Cloud and/or private cloud environments to suit your business operating model – growth, scalability, cost management, giving you a greater level of flexibility, control and agility over how you manage, secure your data and where you store it.

The choice as to whether you should operate within a hybrid or multi-hybrid cloud is a no brainer. Some of the benefits can be seen below:

- Take advantage of competitive pricing to suit your needs.
- Optimise cost savings and operational efficiency – no physical hardware investment (save on Capex), no trained staff to manage hardware, better space utilisation, pay per use, etc.
- More robust resilience and security - access to latest applications, innovation, analytics, etc to better manage your business needs across different geos.
- Benefit from advanced network performance improvements.
- To migrate from one cloud to another is not onerous – an automated migration configuration solution will do the heavy lifting for you with minimal disruption to your business.
- Support your business digital transformation projects with seamless orchestration across public and private clouds so you can take advantage of existing data centres, etc.
- Increase your competitive and strategic advantage – to support different countries judicial restrictions on data management.

Cloud adoption is here to stay - but the companies which are forward thinking have moved beyond the adoption of a cloud to a hybrid multi-cloud strategy giving them more freedom and control to transfer their applications between multiple clouds based on best performance and/or cost effectiveness.

Paul Maritz summarises this well – "Cloud is about how you do computing, not where you do computing". ■


BLOCKAPT™
Simplified.
Smarter.
Integrated.
Automated.
info@blockapt.com
blockapt.com

A national cloud in Switzerland: Challenges and Risks.

Author: Marc-André Ryter

A debate about the importance of digital sovereignty is currently shaking up Swiss politics.

This debate follows the awarding of the design of the "Public Cloud of the Confederation" on April 21, 2021 to the following service providers: Amazon, IBM, Oracle, Microsoft, and Alibaba, i.e. four American companies and one Chinese company. The Chancellor of the Confederation justified the rejection of the national-based providers' bids on the grounds that none of them met the required criteria. This contract, worth some 110 million francs, is currently blocked by a legal appeal filed by Google's attorneys.

It is difficult to understand why the search for a national provider solution was not imposed as a principle, given the sensitivity of this issue and its security implications. It may be seen as a renunciation of digital sovereignty, but in our view, it is above all a risk to the security of the data stored as well as of the transmission of data to and from this public cloud. Such a solution increases Switzerland's dependence of the dominant international companies in this sector. It is also questionable to place as an important criterion to have servers available on 3 different continents. By favouring the market law of supply and demand, without integrating security and political considerations, the Confederation has also *de facto* renounced to establish a needed normative and a strong federal role in the field of data storage. It is clear that a national provider solution would also make it easier to deal with all the legal issues related to the chosen company.

Reaction in Switzerland was swift, with the launch of a popular initiative aiming to amend the country's constitution by requiring the existence of a sovereign digital infrastructure. The Confederation would be responsible for the creation and operation of a digital infrastructure, in collaboration with the cantons, universities, research institutes and Swiss companies. This would ensure that the data hosted in the digital infrastructure is subject exclusively to the Swiss federal law and that this sovereign infrastructure will offer services accessible in all regions of the country[1].

BIO

With a university diploma in Security Policies, after graduating in Political Sciences, Col. Marc-André Ryter is a collaborator of the General Staff of the Swiss Army, for all topics concerning the military doctrine and, since 2018, Head of the Department of Military Constructions. He follows and studies all the technological evolutions which may prove relevant for the Armed Forces and for different operation fields, with a particular aim to adapt the military doctrine.

What seems somewhat intriguing in this case is that the analysis of the risks associated with this state bid was not carried out prior to the contract signing but was planned after it. It is obvious that such an analysis should be carried out before any state bid, in a way ensuring that the strategic consequences of the choice of the company are clearly established.

This article aims to highlight the security issues surrounding this question, and what can endanger the proper functioning of a state and its institutions. To understand the stakes of the challenge, it is sufficient to mention that data traffic on the internet has increased by a factor of 1000 since 2002 and that such data constantly crosses national borders.

The issue of digital sovereignty and a cloud that would remain under Swiss control concerns the security of the data stored. This data is multifaceted: it may concern citizens, but also the country's defence. On the other hand, it will a strong implication on all political, economic (including owners of critical infrastructures) and social actors who would desire to become users of the national cloud. This openness may be of interest to many actors for whom a neutral and politically stable Switzerland is an important key of the country's attractiveness. Its national could therefore become a highly demanded service, and therefore it needs to be secure.

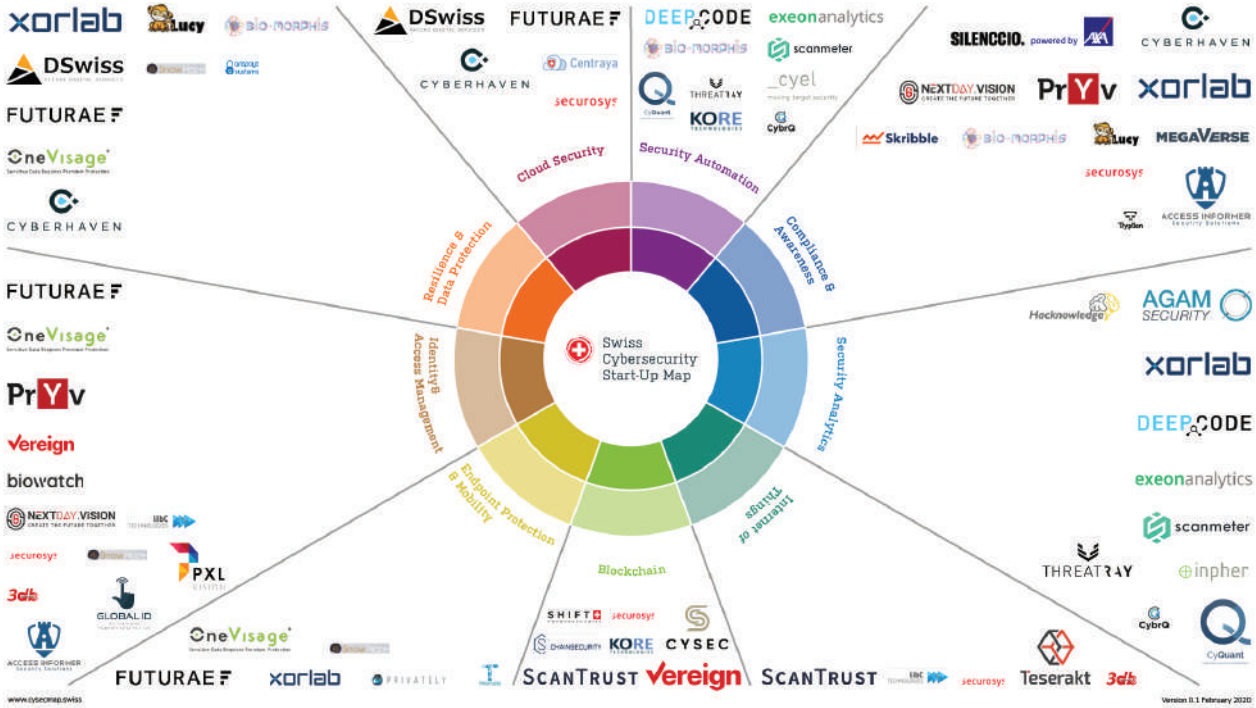
Overall, the control of a federal cloud is really a matter of national security. It is a question of preventing the data of citizens, but also of companies and authorities, from falling into the hands of actors who could misuse them. So, when a cloud is created, it is important to know exactly where the data will be stored, and to be sure that all the necessary measures have been taken to guarantee the security of the data and that there are protocols in place in case the data are stolen or corrupted. And in Switzerland, reactions to a solution that entrusts American and Chinese companies with the task of storing data that potentially concerns all of the country's players are not very enthusiastic... Even more, since Switzerland has the scientific, financial and industrial means to develop a solution that includes secure data centres on its territory and using exclusively Swiss technologies.

SAFESWISS CLOUD

infomaniak

Two examples of 100% Swiss Cloud Providers

Of course, digital security will require massive investments, especially as Switzerland is lagging compared to countries where security is on the top preoccupations of the State and of the main economic actors. The average



The constellation of 100% Swiss Cybersecurity start-ups

awareness level on the challenges of digitalisation is not yet sufficient at all levels, and it is especially the case at the level of the country's political leadership.

Let us therefore return to the issue of risk analysis in more detail. There are indeed very good reasons to call for the inviolability of certain data, as the authors of the popular initiative do. First of all, digital infrastructures have become essential for the proper functioning of almost all societies, and all dimensions within them. A disappearance, corruption or misuse of data can therefore immediately impact the lives of citizens and businesses. It should not be forgotten, however, that the digital infrastructure needed for societies to function properly is not only about data storage centres. Networks are also an important part of this infrastructure. Without a network, there is no data transmission. Moreover, malicious actions can also be implemented via the networks, and not only by direct actions on the storage centres.

A national solution would therefore allow Switzerland to take all necessary measures to increase infrastructure protection on its own initiative and in a quick time, including physical measures such as the use of an army protection system in case of an increased threat.

Secondly, it is also important to avoid dependence on foreign infrastructure, platforms and tools, which, in the event of a sudden interruption in the availability of their services, could also hamper the smooth functioning of the society and the economy, or the country's defence capabilities. It is imperative to avoid the possibility of being cut off from data access, which can happen at any time, for geopolitical reasons or due to economic competition.

In addition, the risks of surveillance or economic and military espionage are to be reduced. An external solution would not provide a guarantee against possible backdoors that would escape Swiss users.

However, Switzerland must also be able to independently and securely ensure its ability to continue the digital transformation of its industry over the coming decades. It must be able to support local innovation and thus ensure a continuity of the competitiveness of its companies. It is essential that the authorities make a commitment to reduce the risk of our country missing this shift and stagnating at an obsolete technological level. In this area, Switzerland must maintain a capacity to anticipate the evolution of risks to in order to propose appropriate solutions to mitigate them.

The country's defence is particularly dependent on digital solutions with a high degree of security. The Federal Department of Defence, Civil Protection and Sport (DDPS) has developed several basic documents to ensure that all its needs in this domain are covered. First, there was the Cyber Defence Action Plan (CDAP) in 2016. Then, due to the quick development of the cyber threat, a new cyber strategy, built on the CDAP, was developed for the period 2021-2024. This strategy is now coordinated within the *"National Strategy for Cyber Risk Protection in Switzerland"* (NCPS).

The DDPS cyber strategy structures the actions within the DDPS into four key areas[2]:

- Governance and Coordination
- Security and Resilience
- Situation assessment followed by immediate action
- Monitoring trends and providing assistance

The identification of existing and emerging risks is a top priority within these documents and clearly highlights the need to develop innovative solutions to effectively counter threats in cyberspace and to ensure and enhance the security and resilience of the digital infrastructure.

Risk management is very important for the armed forces in general and therefore also for the Swiss Armed Forces. The good functioning of more and more control and weapon systems depends on a secure transmission of an increasing amount of data and of their security. The risks of malicious or inadvertent interruption of data flows, as well as those of possible data corruption, are to be taken very seriously. These risks are all the more important as the increasing integration of deep learning processes related to artificial intelligence in military systems could be compromised.

The conflict between Russia and Ukraine, which has been going on since 2014, has shown the importance of digital security for the proper functioning of a country, when facing a high disruptive and destructive potential in the cyber domain.

Of course, it is also a question of avoiding the perception that a Swiss solution, developed under the *aegis* of the Confederation, could be perceived as a possibility for the State to have control over the data, which is a risk in itself. Similarly, the question of the participation of foreign companies, which might be necessary from a technical and financial point of view, will arise. It will then be necessary to determine which would be the acceptable share from the risk point of view.

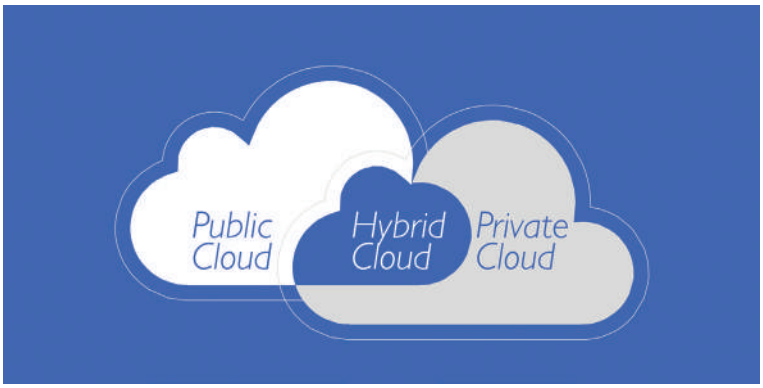
In summary, digital sovereignty, i.e., the ability for Switzerland to fully control what happens to its data, must be based on 4 main elements, which will allow it to control the risks mentioned above. Switzerland needs to know where its data is stored, which software processes it, which legal rules apply and it needs to keep control of the funding. In short, it must first and foremost retain complete leadership over the process of creating its cloud. ■

1 According to the text of the articles proposed in the initiative.
2 Source: https://www.ar.admin.ch/fr/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html, accessed on 15.03.2022 at 0900.

The transition to the cloud: A must for all sectors.

Author: Rossella Macinante

The Cloud is no longer an option for companies, especially those that want to compete successfully and achieve growth objectives, as it is one of the main enablers of new business models and offers the flexibility and scalability that organisations in any sector can no longer do without.



In the Cybersecurity Barometer 2021, the survey conducted by NetConsulting cube on about 80 companies and Public Administration bodies, mainly large ones, it appears that 90% of the sample has implemented at least one type of Cloud service, with a prevalence of hybrid environments (about 51% of the panel).

The healthcare emergency accelerated the migration process for those who had already embarked on it and confronted those who were still sceptical about the cloud with a one-way street, where the cloud was the only way to ensure continuity of service delivery and in some cases even the minimum factors for survival in the market.

BIO

Rossella Macinante is BU leader at NetConsulting cube for the Cybersecurity, Government and Finance areas, with consolidated experience in analysing the technological evolutions that enable the digitalisation processes of companies. For the past 5 years, she has been responsible for the Cybersecurity 4.0 Barometer project, where companies from a demand and supply perspective, discuss relevant cybersecurity issues. The Barometer is also based ,on a survey aimed at providing an exhaustive, constantly updated and complete picture of the level of maturity in the cybersecurity field of the main Italian companies and organisations.

A further 30% of the panel, mainly from the Energy-Utilities, Telecommunications and Industrial sectors, have already migrated more than 50% of their workloads to the cloud, regardless of the model implemented. In addition, a further 42% have already introduced multi-cloud strategies, specifically the use of different providers in infrastructure and platform environments. Again, energy utilities and large industrial companies are the sectors that have most frequently implemented this model.

But even more significant evidence of the disruptive impact of this technology is the fact that migration to the cloud is included in the strategic plans of major Italian companies (Enel, Intesa Sanpaolo, to name but a few), and the term cloud journey is used to indicate an evolutionary path that involves not only innovation of technological architectures, but also a process of organisational change and change management.

Risks to consider

As with all innovative technologies, cloud adoption must take into account the costs and benefits of migration and the areas of concern that, if not properly assessed and analysed, can become critical. One of the main points to consider is cloud security, both in terms of the data that is transferred to the cloud and the governance of the relationship with the cloud provider.

Not surprisingly, the Cybersecurity Barometer panel cited the need for governance tools that enable an end-to-end approach to security as an important issue for 55% of cloud companies.

But it is the protection of data in the cloud that is the main concern for companies, also in view of current regulations such as GDPR. In the Cloud

Security Survey, which was carried out by the SANS Institute on around 300 companies worldwide that use public cloud architectures, data protection, internal expertise, integration and migration issues are the main security concerns.

More specifically, unauthorised access to data by outsiders (56 %) is the biggest security concern. Possible compromise of customer data and information at service provider sites is one of the main risks companies consider when migrating to the cloud.

The risks related to the integrity or unavailability of data may be determined by various factors, including but not limited to: a poor configuration of the environments and the vulnerability of segregation mechanisms; the interception by malicious persons of data in transit from the customer to the cloud provider or between the different sites of the cloud provider; Denial of Service attacks aimed at exhausting the resources of the Cloud

Service Provider, slowing down access to data and services; the loss or compromise of cryptographic keys, with possible unavailability or theft of data.

Other threats to corporate security include inadequate or insecure configuration of APIs (54%), lack of Cloud security skills/training (53%), lack of visibility of what data is processed in the Public Cloud and on which resources (53%), and the presence of unauthorised application components or computing instances (51%).

In addition to technological risks, organisational risks should also be carefully considered. One of the main risks is the risk of lock-in, which translates into the difficulty of changing supplier or re-internalising services. This dependence may be due to the lack of specific skills and resources within the customer or to the use of Cloud Service Providers that widely use proprietary technologies that are not interoperable. In particular, one of the main risks of Lock-in is related to data portability.

Cloud Computing and GDPR

In a contract for the provision of cloud services, the cloud provider assumes the role of external controller with respect to the company or entity storing the data in the cloud, which is the data controller.

The cloud provider, as data controller, shall only be liable for damages to a data subject if it has not properly fulfilled its obligations under the law or if it has acted in a manner not specified in the contractual agreements with the data controller.

A key aspect concerns the security measures implemented by the cloud computing provider. Therefore, before proceeding to use a cloud service, it is necessary to map the data that will be processed externally, in order to identify clusters with different levels of protection.

In this perspective, it will therefore be necessary to obtain the following information from the cloud provider:

- the possible use of storage technologies with (physical or logical) separation of data between the various 'clients' of the provider;
- the possible use of tagging systems to prevent data from being replicated in certain countries or regions;
- the possible use of data encryption and access policy management systems, with access logged;
- the possible use of secure communication systems (SSL/TLS) for accessing data via the browser.

One important aspect concerns data encryption, which is generally provided for data transmission or storage but not in the processing phase, as the data is often used by the platform to feed an artificial intelligence system.

The new National Cloud Strategy

The cloud is one of the fundamental axes of the digital transformation in Italy and of the Public Administration.

Data control, technological autonomy and digital sovereignty, and resilience are the key aspects of the new national cloud strategy, which also ties in with the NIS directive and the National Cyber Security Perimeter.

The Cloud strategy for Public Administration is based on the following strategic guidelines:

- Classification of Data and Services according to three levels: strategic, critical and ordinary. The classification must take into account the estimated damage to the country system that could result from their compromise. In addition, the classification represents one of the main criteria in the choice of cloud provider and service mode;
- Qualification of Cloud Services: to simplify and regulate the acquisition of Cloud services by Public Administrations, from a technical (e.g. operational management, security) and administrative (e.g. contractual conditions) point of view;
- National Strategic Hub: which will have to guarantee adequate levels of business continuity and fault tolerance for strategic and critical Public Administration services. To this end, the operational management will be entrusted to a qualified provider, selected through a European tender, and the infrastructure will be designed in compliance with the data interoperability standards defined at European level, to allow the free exchange of non-personal data between the various Member States by interconnecting their national cloud models.

As one can easily understand, the issue of data and their classification is once again central, since it will determine the type of clouds on which they will reside, and at the same time it is necessary to have precise and defined guidelines to allow the actors involved to make choices in a way that complies with the regulations.

In conclusion, in view of the possible threats and the impact they could have on the business, any process of migration to the cloud must include a risk analysis of the outsourced services that takes into account certain elements, starting with the classification of the data migrated to the cloud in terms of strategic importance for the business and/or confidentiality. It is clear that the essentiality/criticality for the company of each service that is migrated to the cloud is another aspect to be taken into account along with the type of cloud and the service model. A further point of attention concerns the continuity of the risk analysis process that will have to be repeated periodically throughout the report to update the assessment of risks and their impacts.

There is no doubt that the evolution towards the cloud is complex and involves investment in both technology and skills, as well as internal reorganisation of IT and other functions (think of the different skills that procurement and legal departments will need to have), but it is a process that is inevitable because of the benefits it brings and in order to keep pace with market developments. ■

The importance of protecting the Cloud in a post-pandemic world.

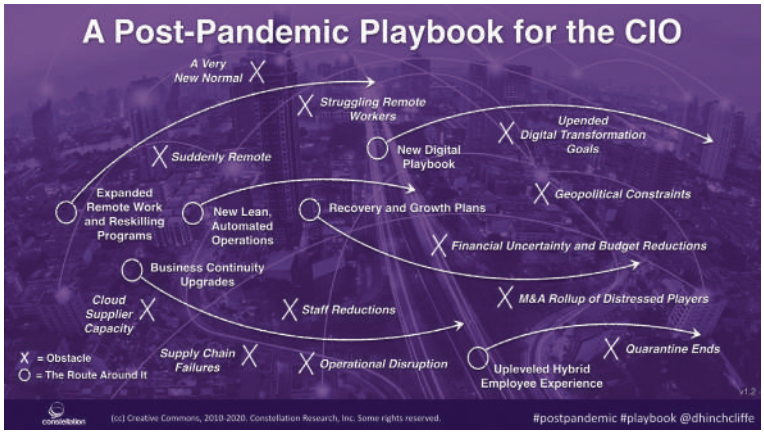
Author: Lisa Ventura

It has been almost 2 years since organisations had to change globally and move quickly to a 'smart' working model due to the global pandemic of COVID-19. While some employees are slowly starting to return to the office, many organisations have now adopted a hybrid model

that allows staff to work both off-site and on-site. This has led to an increasing reliance on cloud infrastructure, which is an essential tool to enable collaboration and business continuity. Cloud security, therefore, is more essential than ever.

Cloud services used to be something 'nice to have', but now they have become a business enabler. Currently, 92 per cent of organisations use public, private or hybrid cloud environments, according to an IDG report.

As well as playing an important role in disaster recovery and operational resilience, cloud computing and infrastructure facilitate the flow of information, making it easier for employees to access what they need and collaborate with others, even from the comfort of their own homes.



But this advantage is also a disadvantage. Information is easily accessible to employees wherever they are, but so are cyber criminals looking to exploit vulnerabilities in the system. With a much larger attack surface on the cloud, there is a great need for robust security controls and a growing demand for experienced personnel in the space. But what is the cloud and how can it benefit your organisation?

What is cloud computing?

Cloud computing is the provision of computing services including databases, storage, networking, servers, storage, software, analytics and intelligence over the Internet ('the cloud') to provide better innovation and resources.

Cloud security varies according to the category of cloud computing used. There are four main areas of cloud computing:

- Public cloud services, managed by a public cloud provider - These include software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS).

- Private cloud services, managed by a public cloud provider - These services provide a computing environment dedicated to a customer but managed by a third party.
- Private cloud services, managed by in-house staff - These services are an evolution of traditional data centres in which in-house staff manage a virtual environment that they control.
- Hybrid cloud services - Private and public cloud computing configurations are combined, hosting workloads and data based on factors such as cost, security, operations and access. The operation will involve internal staff and, optionally, the public cloud provider.

When using a cloud computing service provided by a public cloud provider, data and applications are often hosted by third parties. This is a fundamental difference between cloud computing and traditional IT where most data is stored within a self-controlled network. Understanding your organisation's security responsibility is the first step in building a cloud security strategy.

Security challenges in the Cloud

Since data in the public cloud are stored in a third-party provider and accessed via the Internet, several challenges arise in the ability to maintain a secure cloud. These are:

Data visibility in the cloud - In many cases, cloud services are accessed outside of corporate networks and from devices not managed by IT. This means that the IT team must control the cloud service itself to have full visibility of the data, as opposed to traditional means of monitoring network traffic.

Controlling cloud data - In a third-party cloud provider's environment, IT teams have less access to data than when controlling servers and applications on their own premises. By default, cloud customers are granted limited control and access to the underlying physical infrastructure is not available.

Access to cloud data and applications - Users can access cloud applications and data over the Internet, rendering traditional data centre network perimeter-based access controls ineffective. User access can be from any location or device, including bring-your-own-device (BYOD) technology. In addition, privileged access by cloud service provider personnel could circumvent your security controls.

Cloud security compliance - Using cloud computing services adds another dimension to regulatory and internal compliance. Your cloud environment may have to comply with regulatory requirements such as HIPAA, PCI and Sarbanes-Oxley, as well as internal team, partner and customer requirements. The cloud provider's infrastructure, as well as the interfaces between internal systems and the cloud, are also included in the compliance and risk management processes.

Cloud-native breaches - Cloud data breaches are different from local breaches in that data theft often occurs using cloud-native features. A cloud-native breach consists of a series of actions in which attackers manage to 'land' their attack by exploiting errors or vulnerabilities in a cloud deployment without using malware, 'expand' their access through poorly configured or insufficiently protected interfaces to locate valuable data, and 'exfiltrate' that data to its storage location.

Misconfiguration - Cloud-native breaches often fall on the cloud customer's security responsibility, which includes the configuration of the cloud service. Research shows that only 26% of companies can currently audit their IaaS environments for configuration errors. Misconfiguration of IaaS often acts as a gateway to a cloud-native breach, allowing the attacker to access, move and exfiltrate data. Research also shows that 99% of misconfigurations go undetected in IaaS by cloud customers.

Disaster recovery - Information security planning is necessary to protect against the effects of a data breach. Disaster recovery includes policies, procedures and tools designed to enable the recovery of data and allow an organisation to continue operations and business.

Internal threats - A bad employee can use cloud services to expose an organisation to a cyber security breach.

Cloud security solutions

Organisations looking for cloud security solutions should consider the following when it comes to the key cloud security challenges of visibility and control over cloud data.

Visibility into cloud data - A complete view of cloud data requires direct access to the cloud service. Cloud security solutions achieve this through an API (Application Programming Interface) connection to the cloud service. With an API connection, you can know:

- What data is stored in the cloud.
- Who uses cloud data.

- The roles of users with access to cloud data.
- With whom cloud users share data.
- Where the cloud data is located.
- Where you access and download cloud data from, including from which device.

Control over cloud data - Once you have visibility of cloud data, apply the controls that best suit your organisation. These controls include:

Data classification - Classify data on multiple levels, such as sensitive, regulated or public, as it is created in the cloud. Once classified, data can be blocked from entering or leaving the cloud service.

Data Loss Prevention (DLP) - Deploys a cloud DLP solution to protect data from unauthorised access and automatically disable data access and transport when suspicious activity is detected.

Collaboration controls - Manage controls within the cloud service, such as downgrading file and folder permissions for specific users to editor or viewer, removing permissions and revoking shared links.

Encryption - Data encryption in the cloud can be used to prevent unauthorised access to data, even if that data is exfiltrated or stolen.

Data and cloud application access - As with internal security, access control is a vital component of cloud security. Typical controls include:

User access control - Implements system and application access controls that ensure only authorised users access data and applications in the cloud. A Cloud Access Security Broker (CASB) can be used to enforce access controls

Device access control - Blocks access when an unauthorised personal device attempts to access cloud data.

Malicious Behaviour Identification - Detects compromised accounts and insider threats with User Behaviour Analysis (UBA) so that malicious data is not exfiltrated.

Malware prevention - Prevents malware from entering cloud services using techniques such as file scanning, application whitelisting, machine learning-based malware detection and network traffic analysis.

Privileged access - Identifies all possible forms of access that privileged accounts may have to your data and applications and puts controls in place to mitigate exposure.

Compliance - Existing compliance requirements and practices should be expanded to include data and applications that reside in the cloud.

Risk assessment - Review and update risk assessments to include cloud services. Identify and address risk factors introduced by cloud environments and providers. Risk databases are available for cloud service providers to speed up the assessment process.

Compliance Assessments - Reviews and updates compliance assessments for PCI, HIPAA, Sarbanes-Oxley and other regulatory application requirements.

Why is cloud security important?

According to recent research, 1 in 4 companies using public cloud services have experienced data theft. A further 1 in 5 have experienced an advanced attack against their public cloud infrastructure. In the same study, 83 per cent of organisations said they store sensitive information in the cloud. With 97 per cent of organisations worldwide now using cloud services, it is essential that everyone assesses their security in the cloud and develops a strategy to protect their data. In the UK, the government is playing a central role in the adoption of cloud technology and encouraging organisations to consider adopting it too.

Since its launch in 2013, the UK government's Cloud First Policy has been a flagship technology initiative and an important aspect of the Technology Code of Practice. The policy states that organisations should evaluate cloud solutions before considering any other options. The policy was reviewed in 2019 by government officials and then stated that it would be confirmed in October 2019, demonstrating that the cloud stands out as an approved methodology for modernising the UK's public sector ICT infrastructure.

With the advent of unique challenges such as COVID-19, the public sector needed digital solutions to meet its rapidly evolving requirements. While the immediate goal is to limit human, social and economic loss, operating in the new normal also puts additional pressure on government IT in the years ahead. UK civil servants must use digital channels to inform and deliver services to residents. At the same time, many functions went fully digital during the pandemic, increasing the demand for omnichannel communications.

UK Government's vision for G-Cloud

The G-Cloud framework was developed to help UK government agencies evangelise the Cloud First Policy and source suitable suppliers.

The framework is designed to encourage the use of multi-tenant services shared and managed by multiple groups. Shared resources, infrastructure,

HM Government
G-Cloud

software and information can be provided to a wide range of end-users as a utility, with a pay-by-use model, per user per month. It is dynamically scalable, agile and easy to get in and out of the service. G-Cloud is not a

single entity; it is an ongoing, iterative programme that will enable the use of a range of cloud services and change the way the UK Government procures and manages ICT. By adopting the cloud, government will be able to use and share ICT services more easily and will enable a shift from high-cost bespoke ICT solutions to low-cost standard and interchangeable services. It means changing the culture of government to adapt to the solutions offered by the market and not creating unnecessary customised approaches. The benefits will be:

Many more basic solutions - A range of the industry's best ICT services available immediately so that civil servants can use what they need when they need it and not create duplicate services that cannot be shared.

Flexibility and freedom - The ability, if needed, for departments and organisations to easily change service providers without long procurement and implementation cycles, no 'lock-in' to lengthy contracts and the freedom to quickly adopt better value and state-of-the-art solutions.

Ready and easy to use - Complete solutions already secured for security, performance and service management. Ready-made access that enables cost efficiencies and can be used in conjunction with dedicated on-premise solutions if required.

Low cost - Services paid for by usage, driven by strong competition on price and quality. Transparent costs together with quality and scope of service metrics for easier comparison and control.

Competitive market - A range of service providers constantly improving the quality and value of the solutions they offer, from small organisations providing niche products to large-scale hosting and computer server capacity.

As online interactions increase, digital transformation in government is no longer simply about innovation, but about managing scale, operational efficiency and ensuring value for money for taxpayers, while user expectations, technologies and provider services are changing rapidly.

In the context of COVID19, Software as a Service (SaaS) becomes critical to ensure demand for scalability and reduced costs, as well as easier integration of digital services, automation, efficiency and improved interactions. In a further development in the evolution of cloud computing and security in the UK, the UK government signed a three-year Memorandum of Understanding (MoU) with Microsoft in 2021 to help public sector organisations continue to reap the benefits of cloud computing and enterprise applications.

The Memorandum of Understanding is entitled 'Digital Transformation Agreement 2021' and allows all eligible public sector organisations to benefit from discounts and favourable terms for Microsoft 365, Azure and, for the first time, Dynamics 365 and Power Platform cloud services.

The agreement renews the existing Memorandum of Understanding as a three-year agreement and will run from 1 May 2021 to April 2024. It was negotiated between Microsoft and Crown Commercial Service.

The relationship between the tech giant and the government has increasingly focused on cloud services since the government launched its Cloud First Policy in 2013, which was re-evaluated in 2019 and remains a leading technology policy, according to Microsoft.

This is not the only company to have signed a Memorandum of Understanding with the UK government. AWS signed one in November last year to help accelerate the public sector's digital transformation drive and increase the level of participation among smaller cloud service providers.

In June 2021, UK Cloud signed a memorandum to allow the company to offer its services to the public sector directly or indirectly through its community of partners. The previous month, Google Cloud signed a similar agreement to provide cloud computing to the country's public sector agencies.

Furthermore, the UK's cloud-first policy has been highly influential in shaping the UK government's IT procurement habits in recent years. With over £4.9 billion of cloud purchases made through the G-Cloud procurement framework since its launch in 2013 - 81% of which has been through central government - it has had a fundamental influence on the way the public sector thinks about how it accesses, manages and stores data, encouraging the public sector to adopt more flexible

and cost-effective infrastructure options. The success of the policy is most evident in the way it has significantly expanded the pool of IT products and services available to government organisations, with 45 per cent coming from small and medium-sized enterprises (SMEs).

This has served to promote both cloud adoption and digital public service delivery, working in parallel with the G-Cloud framework to act as a driver to reduce costs and enable scalability within Whitehall and the wider public sector. However, despite its positive impact, the policy is currently under review by the Crown Commercial Service (CCS) and the Government Digital Service (GDS).

How Cloud Security Targets Are Shifting

When the Cloud First Policy was first introduced, it mandated all central government departments to adopt a public cloud approach to technology procurement. Public sector organisations were encouraged to "fully

consider and evaluate potential public cloud solutions before considering any other options" when procuring new or existing services, all to ensure value for money.

To understand the changes taking place, it is necessary to look at the general adoption of cloud infrastructure across multiple sectors. For example, when companies first started adopting the public cloud, they were attracted by various benefits such as the ability to outsource key management responsibilities, gain the scalability needed to support a growing business and, in particular, achieve significant cost savings. Six years on, organisations are reconsidering their strategy due to factors such as unexpected costs and growing security concerns in the public cloud.

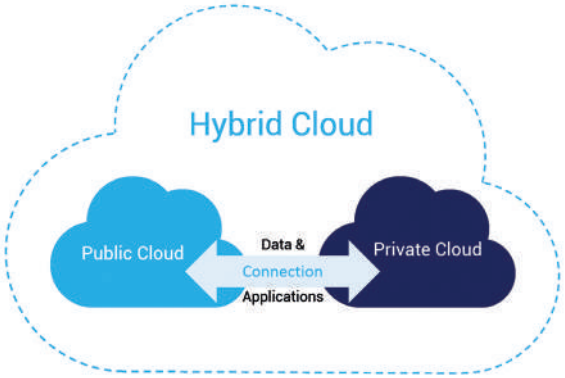
Businesses are realising that a one-size-fits-all approach is not the answer given the complexity of today's IT infrastructure. Today, organisations have complex cost, security and compliance requirements that must be met, leading many to think more carefully about where they store their data. As a result, a hybrid approach that incorporates a combination of local, private and public cloud platforms is preferable.

Cloud Security Must Be Up To Date

The move to a hybrid strategy is a definite trend that is being seen across the IT space and something that the UK public sector is currently recognising.

From a cost perspective, companies in many sectors have realised that costs can rise rapidly in the public cloud, especially if data needs to be accessed regularly. Some providers charge on an access and usage basis, which may not represent good value for money as organisations and their data grow. However, this lack of clarity over the exact costs involved is not an issue with on-premise and private cloud systems, meaning that businesses do not have to worry about being hit with unexpected charges. A hybrid approach offers the best of both worlds with specific workloads configured to ensure that hot data is stored locally and only cold data is moved to the public cloud. This helps control overspending on frequently accessed data.

A hybrid approach can also offer many advantages in terms of security and compliance, both of which are vital for government agencies. Although the public cloud is not inherently insecure, organisations have less control



in ensuring the security of their data. In contrast, on-premise infrastructure provides assurance that data is within the organisation's secure environment and that only a select number of people can access it.

This fuels the issue of compliance, which is a major concern for both the public and private sectors. On-premise systems make it easier for organisations to know exactly where their data resides, which is valuable for compliance purposes and ideal for workloads containing sensitive information such as government documents.

Ultimately, the UK's Cloud First Policy is there to make government agencies aware and confident of the benefits of the cloud. But government now realises that it doesn't need to allocate all its funds to the public cloud to enjoy the full benefits of the cloud, in line with the wider industry trend of hybrid cloud adoption and, consequently, data repatriation.

Government agencies should be free to take advantage of all options to reflect a full range of storage solutions if they really want to achieve cost savings, which is why the focus on hybrid cloud options is unlikely to disappear any time soon. The re-evaluation of the Cloud First Policy is desperately needed and is likely to prove a positive move for the UK government and public sector. ■

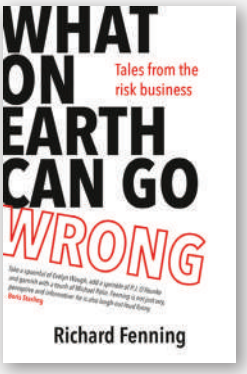
BIO

Lisa Ventura, CEO & Founder of the UK Cyber Security Association, is an award-winning cyber security consultant, and is CEO and founder of the UK Cyber Security Association (UKCSA), an association dedicated to individuals and companies actively working in the cyber security sector in the UK. Lisa is passionate about raising awareness for cyber security, making others more cyber aware in business and helping to prevent cyber attacks and cyber fraud. She is a thought leader, a speaker at various cyber security, technology and IT conferences and events and author of various publications globally.
Lisa is on the Advisory Group for the new West Midlands Cyber Resilience Centre, the board of Think Digital Partners and Cyber Security Valley UK. She is also a strong advocate for women in cyber security, the cyber skills gap and neurodiversity. In 2020 she was named Infosec Superwoman of the Year by CISO Magazine and has won numerous other awards for her work, including SC Magazine's Outstanding Contribution to Cyber Security award.
More information about Lisa can be found at www.lisaventura.com.
Contact details:
@cybergeekgirl and @ukcybersecassoc
https://www.linkedin.com/in/lisasventura/
https://www.facebook.com/lisaventurauk/

It runs in the family: The roots of resilience.

Author: Luca Tenzi

In the last decade, so many articles have been written about resilience and how companies learned to manage, or to surf the crisis and bounce back. As the global footprint of firms expanded, so too have the risks they face daily.



In reference to Richard Fenning's book, "What on earth can go wrong?", we can allude to extended supply chains disruption, technology interdependencies, IT vulnerabilities, mutating viruses, turbulent geo-politics, flat world economics and even weather or earth phenomena all combined to make doing business in a VUCA *(volatility, uncertainty, complexity, and ambiguity)* environment.

But resilience is not a making of the new economy, neither of the 4.0 industry or the start-up culture. Resilience is in the unique gene, the strong roots of the families of entrepreneur and manufacturer that generation after generation have been able to transmit the keys of the realm to the next generation.

Companies like Fabbrica d'Armi Pietro Beretta S.p.A. which headquarter in Gardone Val Trompia, a small valley in the north of Italy, is so distant to the noise of any metropolitan city to make the guest forget its global presence and renowned reputation. Founded in 1526 covering 500 years of history, led by the 16 generations of the same family, this company has witnessed world history. A primary example of resilience and adaptability in five centuries of world history.

Pietro Beretta (1870-1957), the man who made Beretta one of the world's leaders in its domain and the Fabbrica d'Armi in 1960 © Beretta.com

While 500 years with the same family possibly is a world record, there are thousands of companies around the world, created two, three or four generations ago that still run in the family. Resilience is thereof the unmatched ability to pass the family business, from restaurants to motorbike and high value watches, to the next generation of family members while embracing the changes each generation encompass. Resilience runs in the family.

BIO

Luca is currently contractual senior expert at the IAEA (International Atomic Energy Agency, UN-Vienna). Corporate security expert with nearly 25 years of experience in publicly traded companies - has led security operations in diverse environments. His experience spans multiple industries, including, manufacturing, pharmaceuticals, information and communications technology, financial institutions all Fortune 100 and 500 companies. Complemented by experience in specialised UN agencies, including the lead agency for information and communication technologies. Strong advocate for the convergence of physical security and ICT security. Innovative strategic thinker with a proven track record of cooperation, currently working on technology convergence and integration projects. He has published articles on physical, organisational and ICT security, and has been invited to present remarks in industry or geopolitical journals and international seminars presenting emerging or latent business security risks exposing new asymmetric threats. He holds a Post-Graduate degree in Security and Emergency Management from Bocconi University, a Master in Crime and Risk Management from Leicester University, and a DAS in Corporate Risk Management from HEG-SO (Geneve).

Cyber Resilience News

But business 4.0 leaders have lost this generational concept, somewhat resilience 4.0 is a more prosaic business ability to weather the storm and move on. In Raphäel De Vittoris words, it is the ability to face anything and anytime that will make the company sustainable in the current VUCA environment. Sustainable context being prosperous for the investors after the last crisis and before the next.

Therefore, resilience 4.0 in the face of increasing risks and disruptions, summarised in the ability to avoid, deter, protect, respond, and adapt to market, technology and operational disruptions, is becoming a linchpin of profitability, shareholder value and competitiveness and not a legacy to the next generation.

The start-up economy has created several new entrepreneurs, young talents, that regard wealth as the measure of achievement and disregard the longevity as key element of realisation. This business model creates firms that don't last a decade in the same hands, companies that may weather the storm to be sold or dissolved before the next.

The legato that these young professionals leave to the next generation is just an unadorned pile up of wealth with little history attached.

Being evolutionary or revolutionary moment in history, each generation embody aspects of business disruption that will transform societies, for good and evil. We can therefore relate to Nassim Taleb's extremist and mediocratic views and accept that disruptions are genetic factors of doing business while resilience is in the roots of those able to pass on their business to the next generation. ■

Economic security and cybersecurity: From confusion to entanglement.

Author: Stéphane Mortier

A cyber attack...?

Proofpoint researchers have identified a campaign targeting French entities in the construction, real estate and industry sectors. According to the cybersecurity company,

the attackers used a malicious Word document about the General Data Protection Regulation (GDPR). Activating macros to request a URL containing a PowerShell script hidden via steganography techniques in an image. This script leads to the download of the Chocolatey package manager. Finally, the chain of compromise continues to deploy the final payload, the "Serpent" backdoor. The researchers did not identify the final objectives of the attackers. However, based on the techniques, tactics and procedures employed, Proofpoint hypothesises that this is an advanced modus operandi.

BIO

Doctor in sciences of management, associate researcher at the Gustave Eiffel University (DICEN IdF), member of the community of researchers of the Gendarmerie Nationale (CREOGN), member of CMCS.

The following is a brief report in the 23rd of March 2022 edition of the newsletter the ANNSI (National Agency for the Security of Information Systems, ndr.), summarising an article from Proofpoint[1]. A brief analysis can give us the following information:

- the construction, real estate and industrial sectors in France are targeted;
- the argument of RGPD compliance is put forward by the attacker;
- a link to install a package manager;
- the final effect is not known but the modus operandi suggests a targeted attack.

In terms of economic security, the current trend tends to show that a cyber attack is generally the vector of a more complex attack aimed at weakening or disorganising an economic actor. For example, to damage a reputation, to capture data, to hinder a security measure, to disorganise a production line, etc. Can we then dissociate, through this attack, the cyber risk from other risks? The answer is probably no, although purely cyber attacks can coexist with more elaborate attacks.

Economic security can nowadays be considered as a paradigm in its own right, both in strategic management and in public management. Through the above-mentioned attack we propose a draft analysis through this paradigm.

Economic security as a paradigm

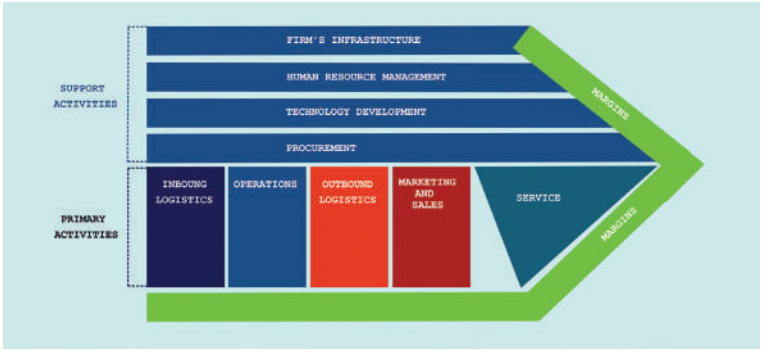
Every company has several objectives: economic, societal and reputational (strategic management). The creation of value involving the competitiveness of the company meets the economic objectives; the contribution to the life of society (employment, taxation, corporate social responsibility) meets the societal objectives; the search for notoriety, compliance, development and increasing the size of the company meets the reputational objectives.

Companies, like all economic players, operate in an ecosystem, in an environment (competitive, normative, technological, social, security,

political, informational, etc.) which is specific to them and which they must master to achieve their objectives. Within this global environment lies the value chain. The value chain contains the various activities of the company that are useful for creating value.

To these activities should be added inbound and outbound logistics, i.e., all the stages linking the suppliers of goods or services to the company as well as all the stages linking the company to its customers, not forgetting the service providers, including banks, insurance companies and even public authorities.

The value chain thus understood constitutes a useful map for all the stakeholders in the creation of value, but also for any malicious actor wishing to harm a company. Indeed, whether at the level of inbound logistics, internal or support activities, or outbound logistics, a multitude of attacks are possible.



Economic predation is today a reality that no longer needs to be demonstrated. In a context of economic warfare, no company is safe from predation or destabilisation. Economic actors, civil society, foreign powers, cybercriminals, etc. are all potential predators, whatever their motives.

The consequences of a breach of economic security are systematically a weakening of the company and therefore a greater exposure to predation. These attacks often have consequences for the cash flow of companies, which is the key to their stability and resilience.

Within the framework of French public policy on economic intelligence (public management), these attacks have been categorised into eight families. These families of breaches constitute a veritable benchmark for economic security. Here are the main characteristics:

- **Physical attacks**, which will mainly concern intrusions, destruction, theft of equipment and materials. For example, a computer intrusion may help the physical intrusion.
- **Disruption and undermining** are actions from the outside. For example, by means of a cyber attack it is possible to slow down the activity of a company.

- The **cyber risks** themselves are of course a considerable risk for companies (DDoS attack, data theft, ransomware,...).
- **Financial risks** do not generally constitute an offence in the sense of criminal law but are tools of predation par excellence. As financial flows are dematerialised, the cyber risk is particularly important.
- The **infringements of know-how** are mainly related to intellectual property issues and therefore to counterfeiting, but also to skills and industrial espionage...
- **Reputational damage** has taken on a considerable dimension with the development of communication media, primarily social networks.
- **Human frailties** are obviously not to be excluded from the spectrum of economic security breaches. Humans are the users (and designers) of digital resources.
- Finally, **consented intrusions** are very important risk factors. Any external service provider constitutes a risk in terms of consented intrusion, including IT service providers (data storage, maintenance, etc.).

This is a reading grid in which cyber risk is omnipresent. From the paradigm to the tool, economic security and the repository of breaches provide a particularly broad vision of the risks linked to the environment of an activity and a key to anticipating these risks.

Analysis of a cyber attack through the prism of business security

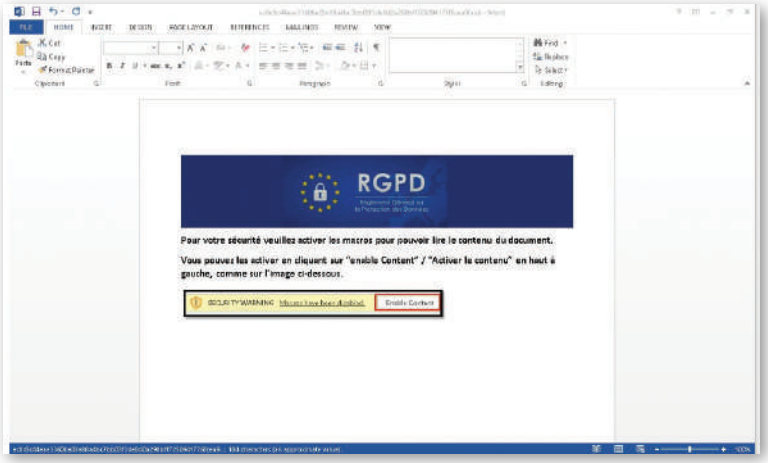
Let's briefly go back to the brief quoted in the introduction to analyse the cyberattack in question with the economic security perspective.

First, the construction, real estate and industrial sectors in France which were targeted. Why these three sectors in particular? At the end of the COVID 19 crisis (*a priori* at the time of writing), the sectors that were particularly affected were those that were not or not very "tele-workable". In other words, the sectors of activity for which either the production chain cannot do without the physical presence of workers: industrial production, construction and catering/hospitality. These sectors are currently in difficulty and could only be kept afloat by public aid (state-guaranteed loans, short-time working, etc.).

The cyber attack in question therefore targets sectors that are already in difficulty (industry, construction and real estate). The predator attacks more easily a weakened or wounded prey, which increases its chances of success.

Second, the argument of RGPD compliance is put forward by the attacker. The arrival of the General Regulation on the Protection of Personal Data (RGPD) in 2018 has imposed compliance on economic actors. This regulation had been little anticipated and many SMEs are still struggling to comply.

Moreover, since 2018, many "RDPD compliance" scams have targeted companies, often using phishing as a starting point. In view of the penalties for failure to protect personal data, this topic is generally taken seriously. By using the RGPD argument, the cyber attacker can more easily convince his victim.



A company that has already been weakened by the crisis will not take the risk of also being sanctioned in terms of personal data management. The attacker's argument seems to be particularly well constructed here and encourages the victim to click on the link that will install malicious software on the user's network or computer.

Third, a link generates the installation of a package manager, i.e. a system for installing, maintaining and uninstalling software. The package contains the computer files, information and procedures necessary to install software on an operating system within a software package, ensuring the functional consistency of the modified system. This is an advanced *modus operandi* and cannot be the work of a simple crook. In addition, a backdoor is also installed, giving remote access to the infected computer. These are the technical aspects of the attack. These tools will allow the capture of data, access to all of the victim's files,...

Finally, the final effect sought is not known but the modus operandi suggests a targeted attack: weakened business sectors, argument of the RGPD and use of fairly complex techniques.

Conclusion

What could be the objective of a cyber attack on companies in vulnerable sectors? In the light of the reading grid proposed above, the modus operandi suggests that data appropriation could be the motive for the cyber attack.

But why in the construction, real estate and industry sectors? The sharp rise in the price of building materials and a property market that continues to grow (especially as a safe-haven) leads to particularly high financial interests.

Collecting accurate data on construction activities and real estate projects is therefore of strategic value not only for the competition but also for the manufacturers of construction materials and even for the logisticians who will transport these materials.

Hence, since construction is a sector that makes extensive use of subcontracting, the stakes involved in positioning oneself on future projects can prove to be very lucrative if anticipated and therefore acquired. As for the industrial production sector, it is subject to a significant increase in the cost of raw materials (remember that, for example, the price of copper reached its historical high in March 2022).

Obtaining information on order books, financial health, the state of stocks, etc. makes it possible to analyse future needs and therefore to position oneself on the supply of raw materials. It would therefore seem, through this rapid analysis and without going into detail, that the objective of the cyber attack is to capture the information necessary for an analysis of the needs in raw materials or materials for the targeted sectors.

Such an analysis, on the French market in this case, would allow the sponsor to establish a strategic plan for the supply of these needs. We would therefore be confronted here with an economic espionage operation that only an analysis through the prism of the economic security paradigm could bring to light. Beyond the cyber attack, a market positioning operation, or even economic predation, is perhaps being played out... ■

1 https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Tools, Culture, Awareness: the challenge of cybersecurity.

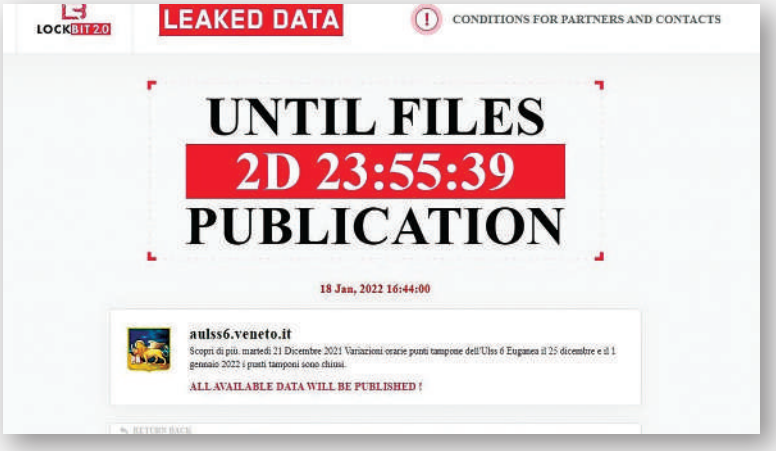
A conversation with Michele Colajanni.

Author: Massimiliano Cannata

"There are no free zones, the organisations are all very exposed, because business runs on digital tracks. We are seeing this in these tragic days when the health emergency has been compounded by the drama of war. Risk runs on a dual track: real and virtual, neither of which can be ignored. Despite the evidence, we have yet to make the cultural leap that would allow us to truly understand that security is a systemic issue, and must be pursued and implemented by involving institutional, political and business players. Michele Colajanni has no doubts: security is a critical term, the development of technologies broadens the areas to be protected, there are no happy islands. Protecting data and information is a must, and no one can avoid it.

Professor, the recent attacks on the healthcare systems of the Lazio and Veneto regions have had a serious impact on the lives of millions of users. **Cybersecurity** ***is no longer a subject for 'passionate' connoisseurs, because it has enormous repercussions on the community. What is your opinion on the subject?***

We should have realised long ago how strategic the issue of security is for the development of civilisation and democracy. The aggravating factor in this phase we are living through is the fact that the 'attackers' who threaten our 'tranquillity' have no scruples whatsoever and are increasingly interested in extorting money as quickly as possible. Hackers, who dominate science, are no longer the original 'romantic' solitary saboteurs, nor are they 'nice and clever' web surfers, as certain literature has long consigned them to our imagination. We are faced with criminal organisations, with criminals selling services to other criminals, forming a protection network that is difficult to counter.



Where does Italy fit into the geography of risk?

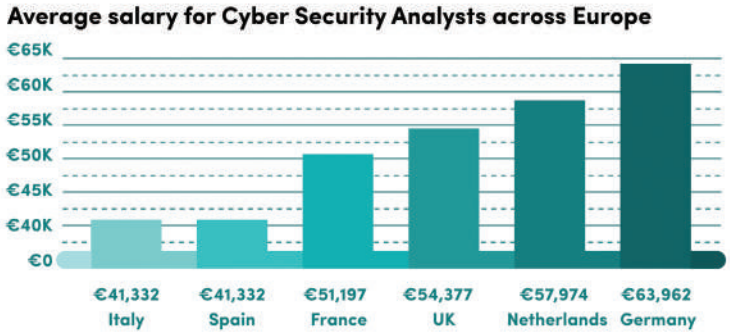
For the avoidance of doubt, let's say that no business organisation or institution in any country in the world can consider itself completely safe, not even in the USA, which is considered a leader in this field. We need to increase our levels of defence, we need tools, of course, but also culture and awareness. Italy is objectively further behind, although the establishment of a cyber security agency should be seen as an important step forward.

There is a lot of talk about public-private partnerships, what is the state of the art in this area?

Beyond the rhetoric, little has yet been "put on the ground". Companies are very competitive, they should learn and open up more to collaborative thinking, and institutions should also take steps in this direction. We need to find forms of invention that act as a catalyst, in order to speed up processes that are still too slow compared to the pace of scientific and technological evolution.

You work at the University, another important player in the game of innovation and development. How do the new generations view a major issue such as the conscious use of the media?

Young people are much more advanced, competent and sensitive than we are commonly led to believe. Let's try to make the most of them before other countries take the best minds from us. As a teacher of cybersecurity, I deal with final-year students on a daily basis, and I find them very motivated. The cold shower comes from there. Our limit remains that of talent management, and without a real connection between the university and the world of work, our words unfortunately remain empty words.



At the Cernobbio Forum last autumn, Minister Colao announced the creation of a state cloud. What will this mean in terms of changing protection standards?

I think the strategy is generally correct. There has been talk for a long time about the cloud for the world of public administration. It is an open worksite that must also find citizens ready to monitor and intervene so that words can be transformed into concrete facts.

Smart working, IOT, technologies applied to work, the world is increasingly populated by info-appliances. What do we need to understand about the 'revolution in progress'?

That we are facing a profound change in production organisations, not the mere replacement of old tools with newer and possibly more sophisticated equipment. The work culture itself must evolve, as must performance measurement. Let us move away from the logic of the time card and start to assess who is really capable of adding value, of giving quality to processes, acting with originality and a spirit of autonomy. All employees will be in the front row in this new season, provided that we manage to loosen the rigid sense of hierarchy to make way for an equal relationship that facilitates discussion on future issues. Security can only benefit from this, because it needs a forum for genuinely sharing experience and expertise in order to become stronger. We are creating the Internet of Things. Certain protection protocols should be respected right from the design stage. Intelligent machines, automated systems, their security is not only a matter of data protection, but of society as a whole. ■

BIO

Michele Colajanni is Chair Professor at the Department of Computer Science, Science and Engineering of the University of Bologna, where he teaches Cybersecurity as well as Scalable and Reliable Services. He graduated from the University of Pisa and obtained a PhD in Information Engineering from the University of Rome «Tor Vergata». He became a researcher at the same university in 1994 and a visiting researcher at the IBM T.J. Watson Research Centre. He has been associate professor of Computer Engineering at the University of Modena and Reggio Emilia since 1998 and full professor since 2000. He has founded several research and training activities concerning computer security and big data analytics, such as the Interdepartmental Research Centre on Security in 2007, the university master's degree in Computer Security and Legal Discipline from 2002 to 2012, the master's degrees in Cyber Defence Governance and Digital Forensics for the Italian Army General Staff from 2012 to 2020. Director of the University Master Course in Security Management from 2010 to 2018, of the CyberLab established with the University of Tel Aviv under the patronage of MAECI, of the Cyber Academy oriented to ethical hackers and of the Master Course in Cyber Security Management at the Bologna Business School since 2018, and founder of the summer camp RAgazze Digitali («Digital Girls»). He carries out an intense training and dissemination activity in national and international venues and collaborates on cybersecurity, cloud and Big Data issues with public administrations and companies in the financial, defence, energy and manufacturing sectors. He is a member of the National Academy of Sciences, Letters and Arts of Modena, a member of the Advisory Board of AIPSA, of the WG «Cyber security» of the AIPCR Technical Committee «Connected and Automatic Driving» of MIT, president of the European Center for Advanced Cyber Security, of the Board of Directors of the *Telefono Azzurro* Foundation and winner of the Unicef *"Ragno d'oro"* award for the category *"Research and Innovation"* in 2017.

Cyber espionage, the highest risk possible for a business. How to prevent it at best?

Author: Laurent Chrzanovski

Industrial and business espionage costs as well as of financial theft are the two main yet missing components of the benefits for assessing cybercrime benefits as well as business losses. The secrecy created around those types of incidents (mediatised only when state-sponsored) is obviously motivated, for businesses, to avoid additional reputation damage and their non-disclosure, from a State point of view, is aimed to avoid loosing jobs by recognising the real weakness of the complete business panorama of the companies activating on its soil.

From a business leadership point of view, we hear the same generic assumptions made for high-tech hacking techniques : *"My company is too small". "My business is banal and not interesting". "My company is not worth the costs of such an attack".*

Far from us to blame CEOs and boards: all the State efforts in the business cyber prevention and awareness domains, since five years, has been focused on personal data, a logically motivated initiative helping companies to

understand the damages and fines they risk as a consequence of the EU GDPR and of the US Cloud Act implementations.

Unfortunately, the over-abundance of data protection awareness materials produced each year is becoming like a huge blinding sun, impeaching to open business leaders' vision to the protection of what is commonly nicknamed "the jewels of the crown". In most of the EU countries, and in particular in the Eastern and South-Eastern nations of the Union, as the major companies are branches of Western EU multinationals, the espionage danger awareness is almost completely absent from State prevention materials.

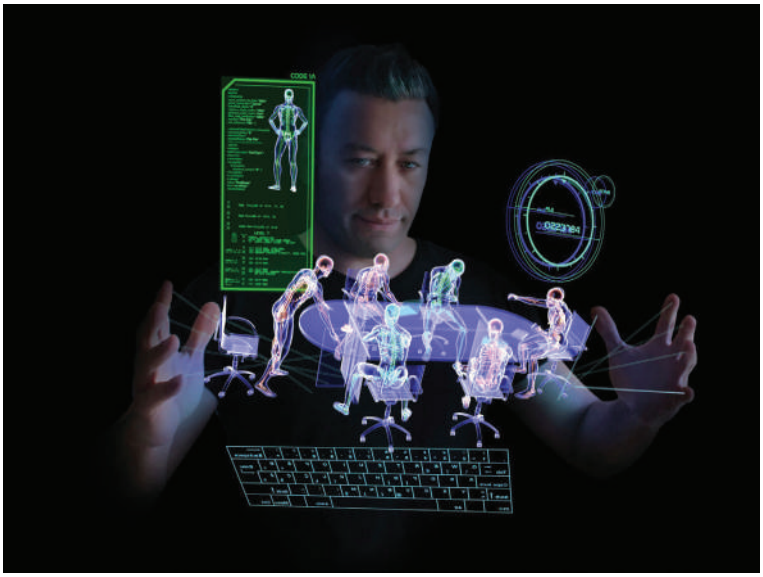
Currently, we are preparing, under the aegis and in collaboration with the Embassy of Switzerland to Romania, for the 1st annual *"Cyber Espionage Awareness Day for Business"*, to be held in Bucharest on 14 June 2022.

As a matter of fact, the Swiss authorities are among the leaders on espionage awareness-raising, along with USA, Israel, South Korea and Japan, a logical consequence for countries where a huge part of the economy is based on innovative companies with enormous R&D budgets, with their core business anchored in some of the world's most economically important domains: military systems, agro-alimentary, chemical, pharmaceutical, high-precision and luxury businesses.

1. What are the aims of espionage for any type of business?

Every single company, in the context of post-pandemic and war times, is interesting. Espionage, when it is not targeting unpatented R&D, is focused on gathering full-scale information on every single part of a business: the complete bookkeeping including suppliers, production and resellers individual costs, the business strategy at short and middle term, the real yearly profit as well as the forecasted innovations or acquisitions and, last but not least, the average health of the business.

The aim for the beneficiary of the spied information is, of course, to know when to buy or to destroy a concurrent. Alas, espionage activities are blossoming in a world where legal companies offer you the data you desire, while exempting you by contract of being legally responsible of any means those companies will use to gather the information you requested, even in the case of using pay-per-service cybercriminal groups.



2. What are the figures of industrial and business espionage?

In his masterpiece *"Managing Cyber Risk"*, Ariel Evans (1) by analysing the costs of both business disruption and data exfiltration (the first type of attacks enabling the second) shows us real numbers which really do scare.

He based his calculations on a huge company, but not a multinational. This reflects the perfect reality of most of the big companies of a country, exactly all those situated under the top-100 ones and above the mid-size or start-up ones.

First, he shows the **Business interruption impact**, as follows:

Crown jewel process	Business interruption loss
Patent management	$0
Clinical trial management	$0
FDA management	$0
Supply chain management	$100,000
HR enrolment	$25,000
Finance reconciliation	$20,000,000
Customer lead management	$20,000,000
Total	$40,125,000

Fig. 1: Evans 2019, Table 3.1, Potential business interruption losses, p. 61

Then comes the data exfiltration impact, where, as we can see, the patent management only doubles the final loss:

Crown jewel system	Data exfiltration loss
Patent management	$50,000,000
Clinical trial management	$25,000,000
FDA management	$5,000,000
Supply chain management	$2,000,000
HR	$1,000,000
Finance	$5,000,000
Customer relationship management	$4,000,000
Total	$92,000,000

Fig. 2: Evans 2019, Table 3.2, Potential business interruption losses, p. 62

Alas, for a business unable to face such an attack, the financial damages are not ending here, as the customers legal actions as well as the regulatory fines will rain:

Crown jewel system	Regulatory loss
Patent management	$0
Clinical trial management	$0
FDA management	$0
Supply chain management	$0
HR	$25,000,000
Finance	$0
Customer relationship management	$400,000,000
Total	$425,000,000

Fig. 3: Evans 2019, Table 3.4, Potential regulatory losses in the US, p. 64

This complete scheme with realistic amounts lets us come back to our article **published in the last issue of this quarterly**, where we quoted to Forbes' top-10 cybersecurity challenges for the current year, where, on 3rd position, we find the insurance costs (2). As a matter of fact, many insurances, whose premiums for coverage have skyrocketed in 2021 are already refusing to accept companies which do not have a strict and comprehensive cybersecurity policy - technological as well as human, starting with continuous awareness-raising training delivered to every single employee.

3. My business is not so huge, what would be my costs?

First, we must stress that in the EU, most insurances are aware that cybersecurity is not a priority for a major part of the businesses. The best is insured in the USA or in the UK, while the others will be refunded by EU insurers at a maximum of 10% of their yearly benefits (not turnover!), hence a useless amount of money when it comes to cover the costs of an espionage attack.

But to speak more concretely , if you have a mid-size EU company, your damages could reach 1/1000 of Evans' case, i.e. 5 million USD, while if your company is small-sided or just a start-up, let us assume it will have to cope with 1/10,000 of the amount, i.e. 500,000 USD. In both cases, in our continent, a bankruptcy of the company is the most probable consequence, a fact mainly caused by the huge reticence of the banks to offer additional loans and hence to allow the business to recover from the attack.

4. How could I reduce at a maximum the risks of being a spied victim?

4.1 Take some parts of the "best of the best" examples:

In Switzerland, the attempted intrusion into the R&D department of one of the country's cutting-edge military systems companies, had a seismic

impact on all other businesses delivering products resulting from long and costly R&D processes (pharmaceutical and chemical companies, etc.) or manufacturing items with very high added-value (luxury watch-makers, top-end industrial components manufacturers, etc.).

The best example is the achievement of one world-known luxury company. It chose the very best IT and cybersecurity companies to build

The costs for insurance is astronomic, reaching more than half a billion USD in Evan's example below:

Crown jewel	Business interruption loss	Data exfiltration loss	Regulatory loss	Total
Patent management	$0	$50,000,000	$0	$50,000,000
Clinical trial management	$0	$25,000,000	$0	$25,000,000
FDA management	$0	$5,000,000	$0	$5,000,000
Supply chain management	$100,000	$2,000,000	$0	$2,100,000
HR	$25,000	$1,000,000	$25,000,000	$26,025,000
Finance	$20,000,000	$5,000,000	$0	$25,000,000
Customer relationship management	$20,000,000	$4,000,000	$400,000,000	$424,000,000
Total	$40,125,000	$92,000,000	$425,000,000	$557,125,000

Fig. 4: Evans 2019, Table 3.7, Cyber insurance quantification, p. 67

its own IT architecture, to segment it with very strict and very small access rules and tested by the best available former black hats. At the same time, it built a brand new headquarter with R&D department with its own servers in atomic-proof bunkers under it. Unsatisfied with all of that, it hired the best former thieves, stuntmen to climb a wall hands free, a real former elite commando and, again, former hackers to make a full scale attack stress-test, which failed.

Of course, no trace of IoT inside the building, outdoor and indoor surveillance is made via top-notch cable cameras, and all the compound necessary tools, including air-conditioning, elevators, fire detection and extinguishing systems are constantly watched by the company's SOC team doubled with physical security employees (not personnel from a subcontracted security company), most of them with licence to wear a fire weapon.

Then, the rules: no meeting without a total check that participants have left all the IoT/IT devices behind, special meetings dealt in anti-G rooms, and draconian rules for every employee: letting one's office or laptop open or giving a password to a colleague result in being fired on the spot. In addition, even the CEO does not have access to more than 2% of any database.

If you reach such level of security, espionage can take place only in its *"neolithic"* form, bribing a highly-placed insider.

The example of the never-signed agreement proposal made more than a decade ago by Switzerland to Germany shows the insider threat at its best. This agreement aimed to tax every German holder of a Swiss bank account and to deliver to the German authorities the yearly amount collected. Yet the richest Länder refused the proposal, obliging the German Federal Government to decline it.

Why? Because at that time (i.e. before Switzerland joined the EU banking cooperation system), most of those regions succeeded, through diverse private agencies, to bribe, up to €10 million+, several IT heads of the two bigger Swiss banks, receiving in exchange a DVD or USB device with the full information of every single of their citizens having an account - and how much was in the account - in the mentioned banks, allowing the law enforcement agencies to bring to justice and punish the fiscal abiding citizens, with all the severity of the German law, hence recuperating amounts of money way higher than the tax proposed by Switzerland.

But as we are not just writing on banks or multinationals, let us summarise the risks a mid or small business will have to deal with, and how to mitigate and even erase some of them.

4.2 Try to adopt the following policies and rules:

Before everything, the CEO and the board must be convinced that drastically reducing the areas of risk is the best guarantee to perform a smooth business without problems, interruptions, fines, and, worse, data exfiltration. In this context, *"Confronting Cyber Risk"*, by Gregory Falco & Eric Rosenbach (2), and "*Inside Jobs: Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore"* by Code42 collaborators (3) makes an interesting read.

The first vulnerability comes from a bad architecture of storage and access management of the IT systems. Every CISO and CSO should carefully review the actual architecture and, using solutions like multi-cloud, limit drastically the number of persons having access to the most critical data.

A careful review and assessment of the security clauses and strengths mentioned in the contract with each IT provider – hardware, software, transmission (cable or wifi) and cloud(s) – should be done as a priority by the CISO and the CSO team, and the companies with weak security levels replaced by trustful one. Ideally, some white hats managing a full, code-source owned, encryption unique to the company would be the best solution to mitigate dangers possible when uploading/downloading/transferring data to clouds or to remote servers of another branch.

The same should be done with the outdoor and indoor surveillance cameras, replacing the webcams with cable ones and hiring physical security personnel directed by a former police or military officer instead of outsourcing the building security and entrance to cheap external companies.

Then, every company should have an exhaustive inventory of its IT means, and this list made available to the CSO. In too many companies, different generation servers and laptops with different versions of OS and software are working contemporarily.

I still remember a talk with the CSO of the Eastern European Country HQ of an Italian major Bank during the "non Petya" crisis. He joked saying *"today I'm the archaeologist, not you! I discovered on floor 7 a still connected Windows XP server and nobody in the IT department could tell me why it was there and more importantly why it's still active".*

BIO

With a PhD in Roman Archaeology obtained at the University of Lausanne, a Postdoctoral Research Degree in History and Sociology at the Romanian Academy of Sciences, and an EU Habilitation to direct PhDs in History and related sciences, Laurent Chrzanovski is Professor at the doctoral School of the Sibiu State University and holds postdoctoral courses within several major EU Universities. He is the author/editor of 32 books, of more than 150 scientific articles and of as many general-public articles. In the frame of cybersecurity, Laurent Chrzanovski is member and contractual consultant of the ITU roster of experts. He founded and manages the yearly "Cybersecurity Dialogues" PPP Congresses (Romania, Italy, Switzerland), organized in partnership with the highest international and national authorities . In the same spirit and with the same partnerships, he is co-founder and redactor-in-chief of the first cyber security awareness quarterly journal, Cybersecurity Trends, published in Romanian language since 2015, with English and in Italian versions since 2017. His main domains of study are focused on the relationship between the human behaviours and the digital world as well as the assurance of finding the right balance between security and privacy for the e-citizens.

In the same domain, the compulsory daily check, by your SOC, of vulnerabilities on trusted organisations (such as the Alerts page of the Singapore CerT) (4), hence knowing about problems before a patch is delivered by the vulnerable soft/hardware producer.

The same, easily hackable Wifi-connected multitask printers, as well other wireless connected shared devices should ideally be banned and replaced /reset on the good old cable mode.

Other compulsory policies, which have to be preceded by awareness raising talks should include :

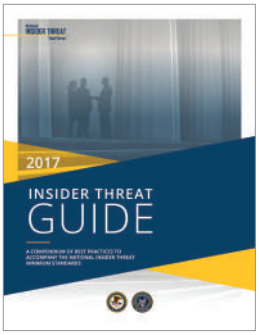
A. Interdiction to surf the internet via the IT tools provided by the company – at least for each decision-maker of each department of the company, in addition to the CEO and the board members. This is a particularly sensitive issue and cannot realistically be implemented to all employees as studies demonstrated that impeaching people to access social networks is a factor which can, alone, motivate an immediate demission and a job change in favour of a company allowing this practice.

B. Constant verification by the SOC of the credentials of all the employees and of the data accessed. Of course, the ***immediate revocation of credentials belonging an employee who quits is key*** . Many companies forget this practice and studies revealed that former employees had their access privileges during 3 to 6 months after leaving a company!

C. Interdiction of entering well-established areas or departments of the company with any personal IoT or Smart device. Above all, no smartphone, no IoT, no IT during strategic/bookkeeping/R&D meetings. This simple solution avoids the most basic espionage tool, as recent studies estimate up to 2 on 10 smartphones of essential employees in interesting companies have a voice spyware installed, enabling hackers to hear everything said by everyone around the person wearing the infected smartphone.

D. If the country's law allows it, **constant verification of all employees' mails sent via their company address** as well as (again if possible by law) a **constant monitoring of their acquaintances as well as their posts on social media**, in particular on LinkedIn.

A study made by Bitdefender twelve years ago, on a mix of 2000 IT and IT security employees accepting a new "friend" on this media showed that after half an hour conversation, 10 % disclosed personal sensitive information, and, much worse, two hours later, 73 % of them siphoned what appears to be confidential information from their workplace, such as future strategies, plans, as well as unreleased technologies/software. Far from being stopped, this phaenomenon is happening now also on Facebook, Google+ and, the cherry on the pie, recent studies show that most "tailor made" fake jobs offered on LinkedIn contain links delivering some of the most sophisticated malwares and spywares of the moment.



E. Behavioural analysis of the employees with access to sensitive documents should be performed in a regular way. Alas, in a world where most employees and even CEOs will work for at least ten different companies until their pension, most insider threats and direct harmful actions (stealing confidential information and sharing it everywhere) ***are perpetrated by employees just as an act of revenge following conflictual relationships with colleagues or direct superiors within the company itself***

For this precise and crucial topic, the USA has created an extremely important tool for businesses: the National Insider Threat Task Force (NITTF) (5) , which delivers constantly extremely pertinent analysis, tools , video and web tutorials as well as reports.

If a company succeeds in adopting all those basic recommendations, and to implement the correct policies mentioned, then it will be safe from 90% of the most common espionage acts, remaining vulnerable only to brute force zero-days tailor-made attacks on the core IT system, extremely costly to perform hence reserved to extremely high-value goals.

In addition, companies should be ready, with some additional actions, to obtain the ISO/NIST/BSI certifications making it be eligible for a US/UK insurance covering all costs in case of an attack without any insider fault, mistake or betrayal. ■

(1) Ariel Evans, *Managing Cyber Risk*, London-New York: Routledge, 2019
(2) Gregory Falco, Eric Rosenbach, *Confronting Cyber Risk. An Embedded Endurance Strategy for Cybersecurity,* New York, NY : Oxford University Press, 2022
(3) Joe Payne, Jadee Hanson, Mark Wojtasiak, George Kurtz, I*nside Jobs: Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore*, New-York: Skyhorse, 2020
(4) https://www.csa.gov.sg/singcert/Alerts
(5) https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

BLOCKAPT™

Digital Central Nervous & Intelligence System .... **Enterprise Connective Fabric**

COMMAND & CONTROL ■ **ANALYSE & ACT** ■ **CONNECT & MONITOR**

info@blockapt.com

blockapt.com

Business Cryptography Risk.

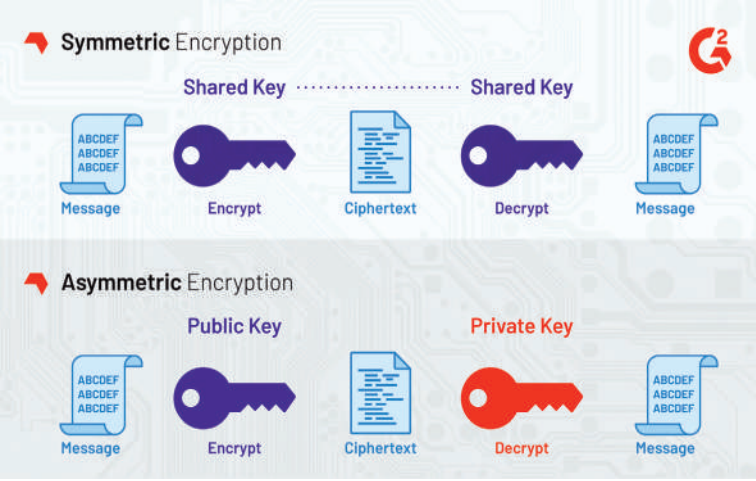
Author: Sunny "Dos" Dosanjh

Organisations around the globe are continually strengthening their cybersecurity posture and mitigating technology risks that negatively impacts their business. These technology risks include public cloud migrations, 5G for Industry 4.0, Business Email Compromise and a host of other technology nuances that exposes the organisation for a cyber-attack. One sub-topic of the cybersecurity posture that is often overlooked, due to its effectiveness, is the cryptography posture.

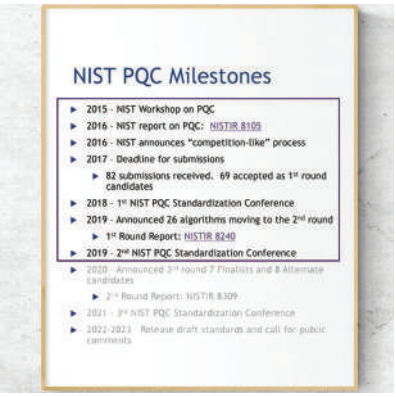
A cryptography audit, of any organisation that processes hybrid workflows, highlights the multiple transaction points where cryptographic methods are utilised. These workflows range from datacenters to public clouds, integrations with third party services and IoT endpoints. The cryptography selection, whether encrypting, hashing, or tokenizing, always includes multiple complex inputs that influence the decision-making process. For

example, data residency laws, industry vertical market regulations and the organisations propensity for risk tolerance all play a part in the final selection.

To date, it has been a fairly straightforward choice to build upon methods such as asymmetric or symmetric key encryption or a combination thereof. An organisation can review an application requirement such as Salesforce data search & sort and associate an encryption scheme that meets their objective. The organisations propensity towards risk will determine which encryption method is authorised or if an advanced solution is required to support data tokenization. We'll classify this method and supporting cryptographic approaches as "Classic Encryption."



Enter into the room, Post-Quantum Cryptography or PQC for short. If an organisation does not have an up-to-date cybersecurity cryptography dashboard for Classic Encryption, then they will have a challenging time implementing PQC. This will expose an organisations understanding of their cryptographic risk and preparedness for assessing the forthcoming Quantum-Safe encryption standards. The risk is extended to anyone, customers, partners, or employees, who interface with the business using technology stacks comprised of data, applications, networks, and devices. Although the NIST (National Institute for Standards and Technology) PQC evaluation and selection process may take until the end of 2023 or early 2024, the proof of technology trials are underway with organisations that are considered early adopters.



Whether you're a Fortune 1000 Company or a Small & Medium Business, 2022 will become the year that decisions will be made to embark on a security apparatus that is Quantum Ready and Quantum Safe. Although currently, the majority of the Managed Security Service Providers, technology vendors and consulting firms that I conversed with at the largest North America Channel Partner Expo (Las Vegas, April 11-15, 2022) were focused on incident detection and reporting. This was primarily due to the new Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA.)

BIO

Sunny is the CEO of DUSA SPACE. He is a technology veteran working in Silicon Valley, California for the past 25 years as a network engineer, solution architect and cybersecurity leader. During that time, he has worked for Sony, Cisco, and numerous cybersecurity startups such as BlueCoat Systems, CipherCloud and Appcito. He currently provides consulting for Post-Quantum Cryptography, Salesforce & Multi-Cloud data, application, and network security. His career began in the US Air Force and he earned his Bachelor of Science, Information Systems from San Jose State University. Today he volunteers as the Chaplain with the American Legion in Santa Clara, California and as a Royal British Legionnaire in Isleworth, London.

The act was signed into law on March 15th, 2022, by the President of the United States. The White House also released a National Security Memorandum this past February stating that all US Federal Agencies had to report their roadmap on how to transition from Classic Encryption to Post-Quantum Cryptographic supported solutions.

In order to mitigate the business and technology risks associated with Classic Encryption and forthcoming PQC services, organisations will require an assessment of their cryptography posture. This assessment will require the inclusion of new functionality that supports Command and Control capabilities that can orchestrate, automate, and remediate Classic services. The combination of these services will usher in a new wave of Quantum Managed Services and assist in "Building the Bridge" from Classic Encryption to Post-Quantum Cryptography. ■

Single Password Authentication should be banned: Here are 5 reasons why.

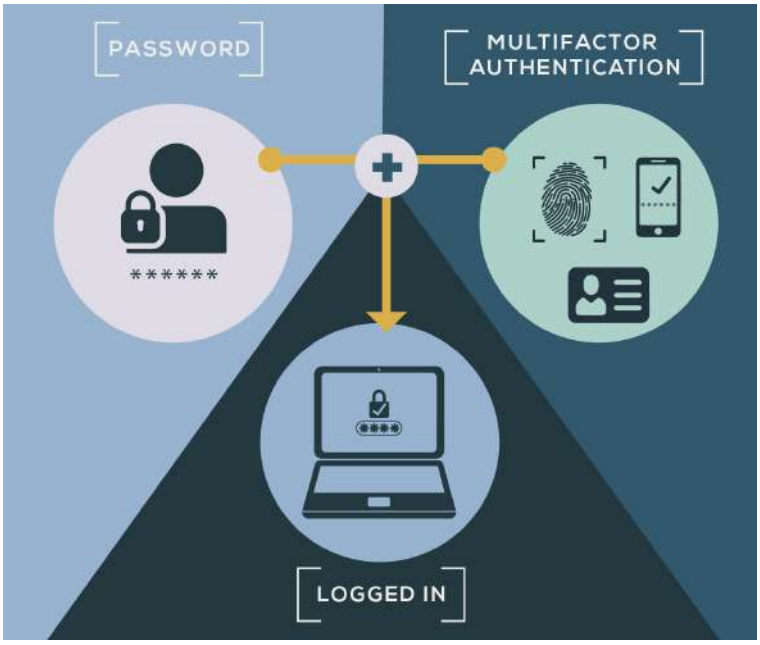
Author: Marco Essomba

I use passwords a lot. I have different types of passwords. From strong, mega strong, and paranoid strong. Some I can remember some I can't. It drives me mad sometimes.

Whether you like passwords or not single-factor authentication (SFA) also called single-password authentication, remains one of the most common amongst the first line of defence used by various online systems to protect against unauthorised access to applications and data.

Single-password authentication is one of the top-ranking attack vectors used by cyber criminals to break into online systems, opening up the threat landscape to cybercriminals and exposing businesses to manage financial, legal and reputational risks.

My view is that single-password authentication should be banned worldwide. All publicly accessible online systems that rely on single-password should be forced to use at least one form of strong multi-factor authentication (MFA). In this article I cover 5 reasons why.



The growing threat of Phishing, Ransomware, and Advanced Persistent Threats:

With the rapidly growing number of sophisticated cyber-attacks such as Phishing and Ransomware, single-factor authentication has had its day. One way to fight back against the rising cyber-attacks is by using strong multi-factor authentication. It must be widespread and used as the most basic type of authentication mechanism. Unfortunately, many service providers and organisations still rely on single-factor authentication as their preferred authentication mechanism for online systems connected to the Internet. This is very bad. This is how businesses are exposed to risks unnecessarily.

Here are 5 reasons why.

1. Humans are naturally 'lazy' when it comes to passwords

When we are challenged to create a password, we often choose something that we can remember easily. That usually leads to a weak password. Using password generators software such as LastPass or Norton Identify Safe can help to create very strong passwords. However, various online systems still do not enforce strong password policies which means users can get away with creating very weak passwords.

BIO

Marco Essomba is the Founder & CTO of BlockAPT – a UK based innovative cybersecurity company.
An influential thought leader in cybersecurity with almost 2 decades of working with some of the largest and well known institutions. Marco's passion, expertise and knowledge has culminated in the design of the unique central management, command and control BlockAPT platform which allows businesses to stay ahead of cyber threats 24/7.
Marco is often called upon as a panellist at cybersecurity conferences and has been a host ambassador at CyberTalks, one of London's largest cybersecurity events. With 16,000+ followers on LinkedIn and 35,000+ on Twitter, he is sought after for his quick problem-solving approach and helping businesses futureproof their security infrastructure.
To find out more about BlockAPT, please visit https://www.blockapt.com
To find out more about Marco Essomba, please visit https://www.linkedin.com/in/marcoessomba/ or https://twitter.com/marcoessomba

2. Computing power is increasing dramatically. Password-cracking tools are getting more powerful

With the dramatic increase in computing power, password-cracking tools are now widely used by cyber criminals. Such tools are used to guess and break passwords very quickly using brute force computational algorithms. And with Quantum Computing, this power will increase exponentially allowing password-cracking tools to break even the strongest password in a very short period of time.

3. Some service providers still store unencrypted passwords

We hear in the news every day about various online systems breached and personal information stolen. One such case was Facebook in March 2021 where 533,000,000 user records from 106 countries were posted on a hacker forum. The leaked information included user locations, full names, biographical information, phone numbers, and email addresses. This information was discovered when a user in the hacking forum promoted an automated scraping bot that could extract phone numbers for hundreds of millions of Facebook users.

4. Password renewals frequency

One way to keep your password safe is by changing it on a regular basis. Various online systems are enforcing this mechanism to strengthen security. However, forcing users to change password at short frequency leads to password fatigue. Unless strict passwords policies are enforced, users may often re-use previous passwords for convenience.

5. Password fatigue

Too many passwords. Too many online systems. Users are feeling the password fatigue. Many organisations are increasingly implementing Single-Sign-On (SSO) to allow users to login once using a single-password and then gain access to several online systems using a chain of trust. However, if the initial password used to gain access is weak, the overall system is also weakened in the process.

Conclusion:

With the increasing number of cyber-attacks against all types of organisations worldwide, single-factor authentication (SFA) also called single-password authentication remains one of the most widely used mechanisms to protect various online systems against unauthorised access.

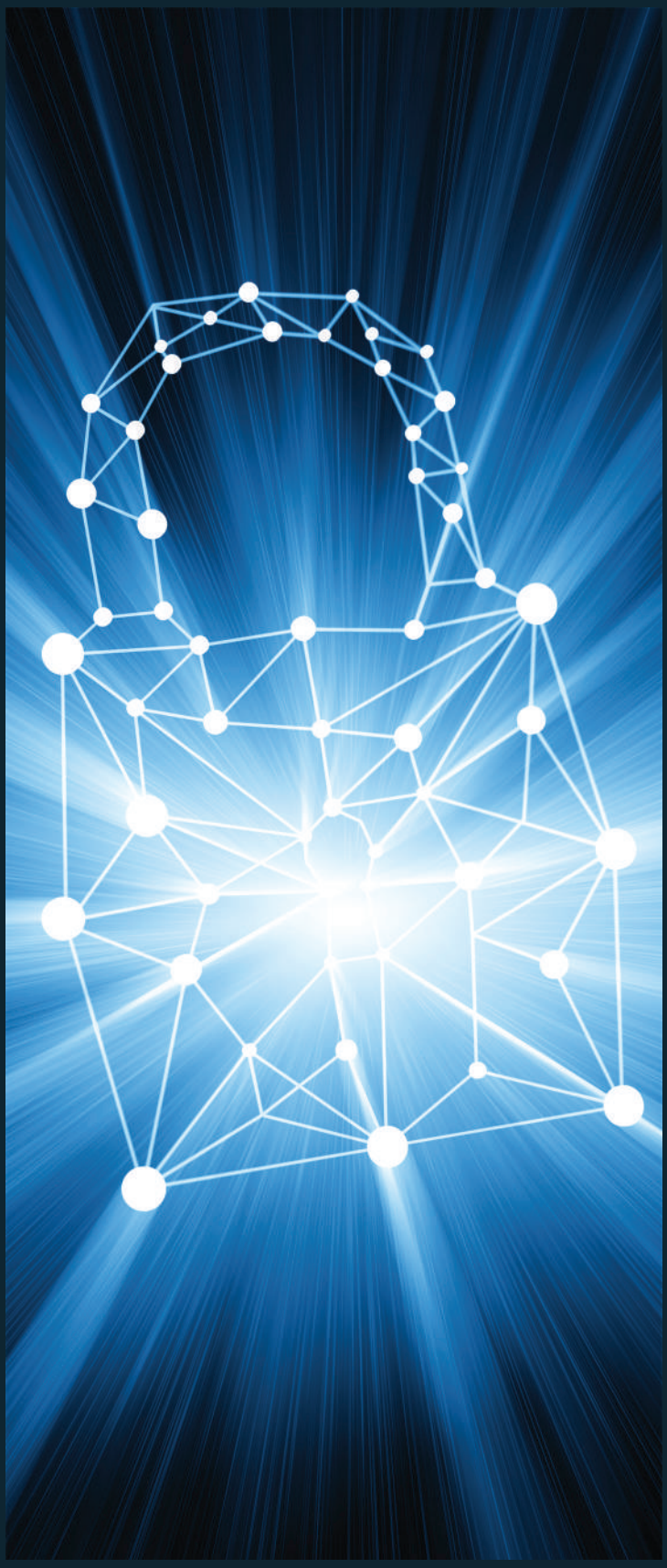
Relying on single-password authentication alone is bad practice.

I argue that it should be banned completely.

All online systems accessible from the Internet should be forced to use strong **multi-factor authentication (MFA)**. This will greatly reduce the rapidly growing number of cyber-attacks worldwide and help mitigate the risk exposure of businesses.

MULTI-FACTOR AUTHENTICATION

Cybersecurity Trends



A publication

web for your business
swiss webacademy

edited by:

BLOCKAPT™

Redaction:
Laurent Chrzanovski and
Romulus Maier †
(all editions)

For the UK edition:
Raj Meghani

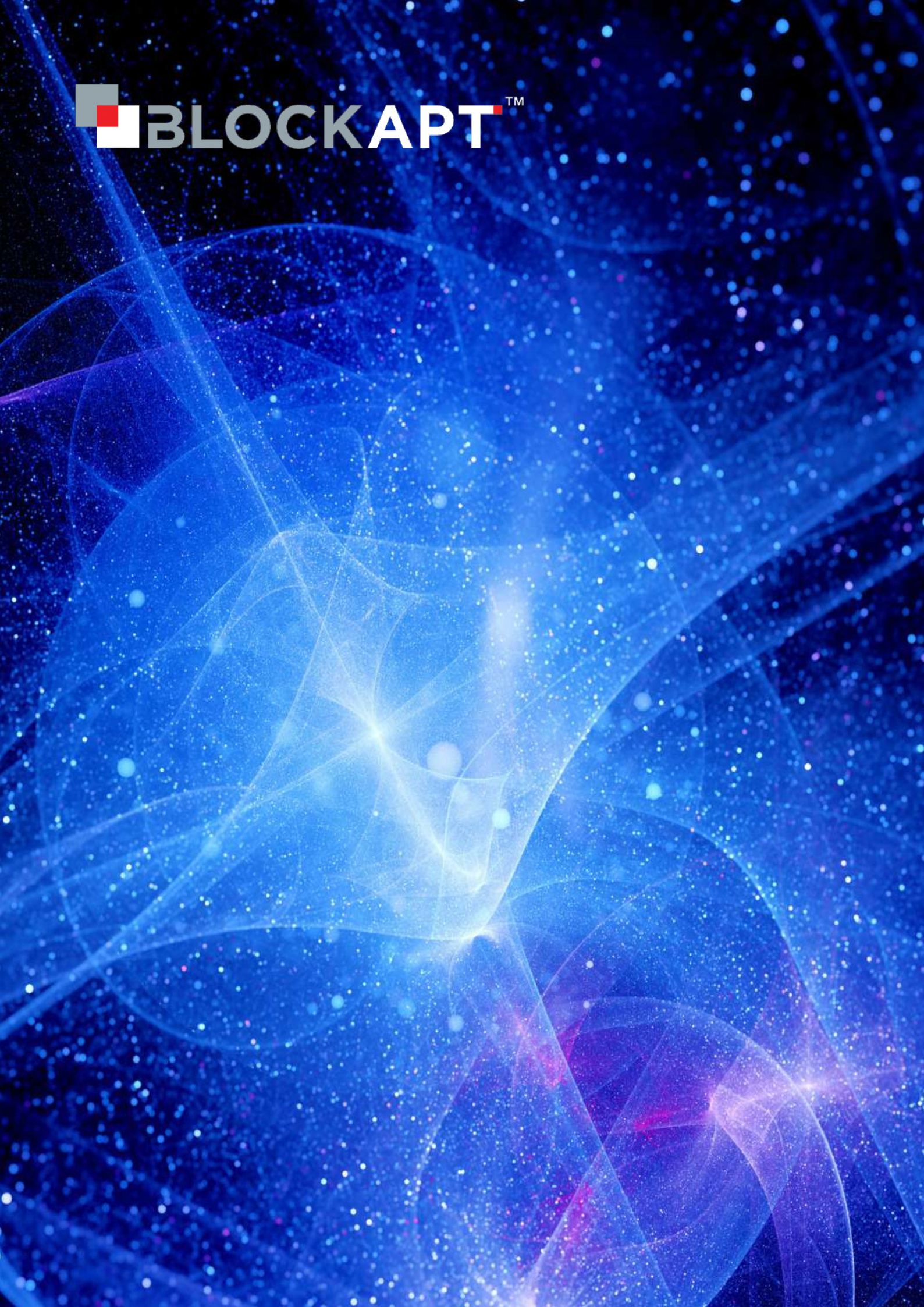
Translation and proofreading:
Laurent Chrzanovski, Raj Meghani

ISSN 2559 - 6136
ISSN-L 2559 - 6136

Addresses:
Swiss Webacademy - Str. Şcoala de Înot
nr.18, 550005 Sibiu, Romania

BlockAPT Limited
14 East Bay Lane,
The Press Centre, Here East,
London. E20 3BS
United Kingdom

www.swissacademy.eu
www.cybersecurity-dialogues.org
www.blockapt.com


BLOCKAPT™