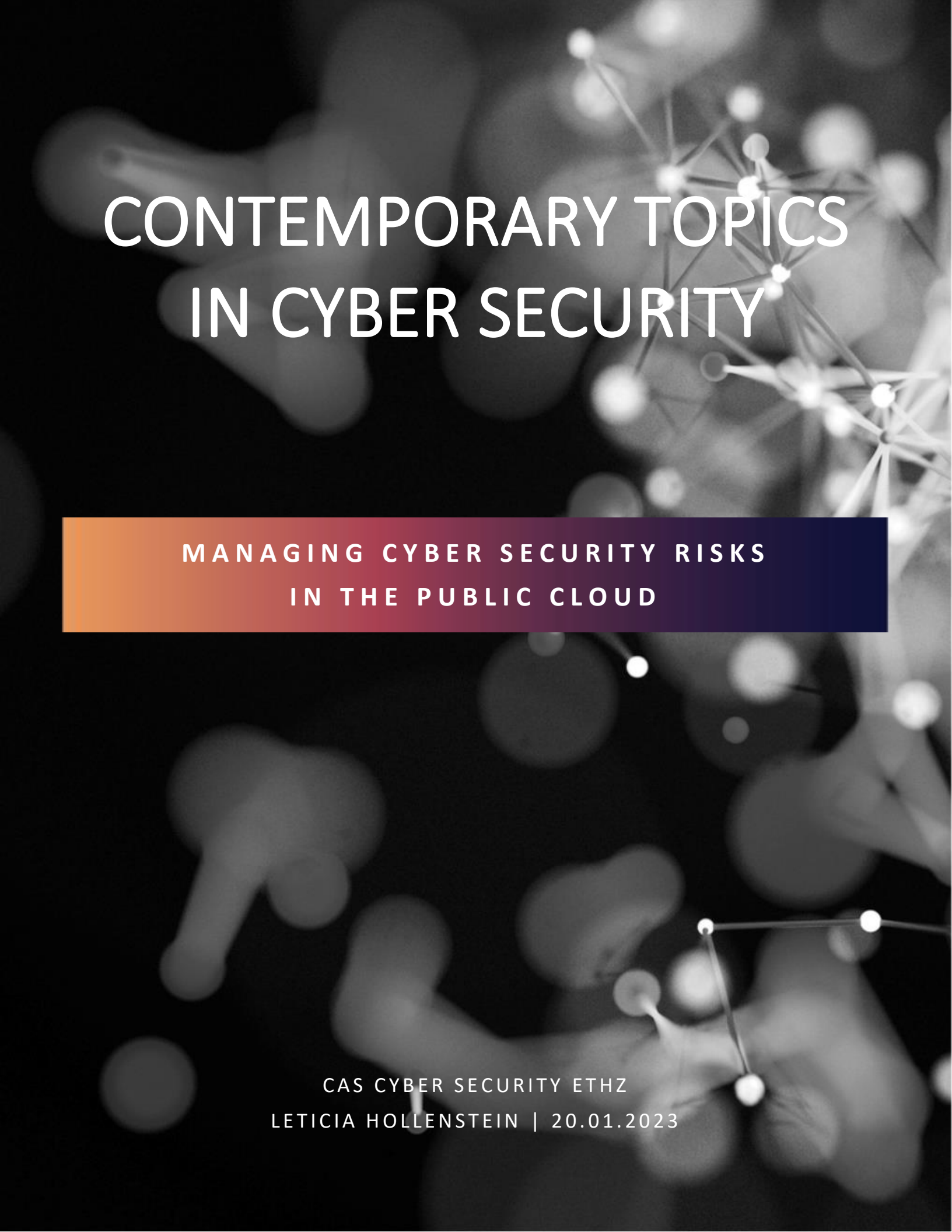

CONTEMPORARY TOPICS IN CYBER SECURITY

MANAGING CYBER SECURITY RISKS IN THE PUBLIC CLOUD

CAS CYBER SECURITY ETHZ

LETICIA HOLLENSTEIN | 20.01.2023

SUMMARY

Public cloud strategies are widely adopted nowadays, even by organizations that are risk averse. The benefits of flexibility, scalability and efficiency are well-known, but the secure execution and management of public cloud environments is often inadequate due to a lack of skills, tools, and processes, resulting in an increased risk exposure.

A risk strategy in line with the organization's risk appetite is only the first step and must include a balance of trust and control, taking ownership of responsibilities as well as building sustainable cyber resilience.

This paper discusses how to manage cyber security risks in a public cloud environment, covering the different service and deployment models in cloud computing, the concept of risk management, and existing mechanisms and tools to mitigate risk. It also provides an outlook on emerging cloud security innovations and considers other factors that may impact cyber security risks today and in the future.

TABLE OF CONTENT

INTRODUCTION

“Security is a risk business. We don’t secure everything and everywhere, otherwise business wouldn’t get done. Focus your security resources on the pieces that add the most value to your organization, so you ensure this value is protected.”

CISO, Cisco Security Business Group

If you had to leave your burning house immediately and you could take with you only a few belongings, what would you rescue? Apparently, these objects or very valuable to you and you would protect them above all. Now put yourself in the shoes of a company and replace your personal belongings with the digital assets that add the most value to the organization. Security resources need to be focused exactly on the protection of these assets. As security resources are limited and at the same time cyber security risks are tremendously growing, you better choose wisely. An appropriate cyber security risk management strategy will assist you in determining what needs to be secured and how to secure it.

Organizations are struggling with the speed of digitalization and the complexity of the security landscape. They are expected to optimize their business while being cyber resilient at the same time. Public cloud computing is one of the disruptive phenomena that rose extremely fast in the last decade, allowing businesses to be more agile, innovative, and cost-effective in our fast-paced world. The pandemic and its related need for flexible and digital processes gave another strong boost to the adoption of cloud solutions during the last two years. Although cloud computing comes with a lot of benefits, for many organizations it is a new technology and a new way of handling their business and processes. It also brings additional cyber security risks that must be considered and mitigated.

We should ask ourselves:

- Which is the IT environment and security strategy that best suits our business needs?
- How should we balance control versus trust in a cloud service provider of our choice?
- Who is responsible and accountable for security in a public cloud environment?
- What can be done to mitigate cyber security risks in the public cloud?
- Which emerging technologies will considerably contribute to the automation and improvement of our security posture?
- How do we personally feel about this topic?

To get answers to these questions, we first need to build a common understanding of the important concepts that matter for the present paper. A deep dive into the notion of cloud computing with a special focus on public cloud is our beginning. Then, we clarify the idea of risk management, especially for cyber security risks. This baseline will give us the common ground for digging deeper into the topic of how to manage cyber security risks in the public cloud. We are going to introduce some approaches and ideas on how to tackle potential challenges, mitigate risks and build cyber resilience. While looking at the possibilities the technologies currently offer for a better security posture in the public cloud, we then also take a glimpse at the future trends in this field. Finally, the view is widened by considering the personal thoughts of the author before closing the paper with a conclusion.

CLOUD COMPUTING

First, it is important to have the same understanding of the term "Public Cloud" before we can start moving forward and concentrate on its relationship with cyber security risks and how to mitigate them.
Cloud computing can be described as a transformative and disruptive way of digital processes, including new technologies, operating models, service models, business models and many more specificities. In the last decade the use of cloud computing has grown tremendously, equally for business and for private use. It offers potential benefits such as flexibility, scalability, and efficiency. It can also bring enhanced security, if implemented and managed correctly – we will come to this challenge later.

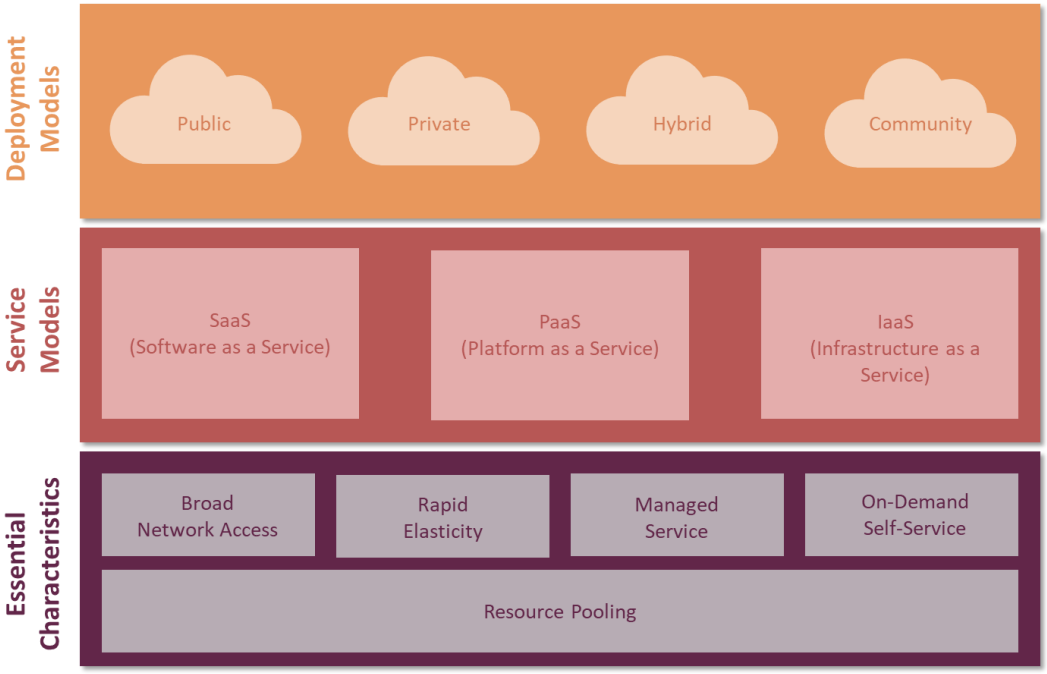

Figure 1: Introducing Cloud Computing (Source: Own illustration inspired by CSA report)

Cloud computing is typically characterized by some main characteristics, can be accessed through different service models, and used within a variety of deployment models (see figure 1). We count beyond the **essential characteristics** of cloud computing the resource pooling of computing services hosted by a cloud service provider. From there, every cloud customer can use these resources on an on-demand self-service. He doesn't need any direct physical access to the infrastructure but only a network to access the service. Thanks to rapid elasticity, every cloud customer can adapt the use of his resources very quickly and pay only for what he currently uses. The underlying services are fully managed by the cloud provider and charged to the customer on a consumption or licensing basis.
We can further differentiate between three main **service models**, namely software, platform, and infrastructure as a service. Going from providing a full application (**SaaS**), the underlying application platform (**PaaS**) or only the computing infrastructure itself (**IaaS**). The service model chosen has a major impact on the management of the technology and the related responsibilities, also regarding security.
We can further introduce the four most frequently seen cloud **deployment models**. Starting with the **public cloud**, where the cloud infrastructure is shared and made available publicly, so to everyone who wants to use and pay for it. Whereas in a **private cloud** model, the cloud infrastructure is exclusively reserved for a single organization. It can be managed by a third party or by the organization itself, either on-premises or off-premises. The **community cloud** is an extended private cloud allowing not only one organization but a specific community consisting of multiple defined organizations to share the cloud infrastructure. In a **hybrid cloud** setting, the customer uses a mix of service models, potentially including also an on-premises infrastructure, meaning computing resources owned and operated by his own.
Depending on the business model, the industry, the processes and requirements, everyone can choose the service and deployment model that best fits his needs. In the following we will focus on services provided in a public cloud infrastructure by a cloud service provider.

SHARED SECURITY RESPONSIBILITY

Let's consider a scenario where a cloud customer uses cloud services from a solution provider in a public cloud deployment model. He can still decide between the different service models SaaS, PaaS, IaaS and can of course also use all of them at the same time depending on the specific use-case. Security in the public cloud basically contains the same areas as security in a traditional setting. The big difference between the two worlds is the nature of security risks, the roles, the responsibilities, and the implementation of security controls. We find the so called "**shared responsibility model**" between the cloud provider and the cloud consumer (see figure 2). In the public cloud, the security responsibilities are shared between the two parties and the area of responsibility depends on the service model. Moving from the left side with the SaaS model, where the cloud provider has more security responsibilities towards the right side with IaaS, where in contrary the cloud consumer owns most of the security responsibilities. Looking at SaaS, the cloud consumer can only manage and access the use of the application but none of the underlying architecture of the application. Thus, the cloud provider is responsible for most of the security in this service model. In a PaaS model, the cloud provider is only responsible for the security of the platform, the consumer is himself responsible for everything he implements on the platform (e.g. application architecture and related security configuration). Third, with IaaS, the cloud consumer owns all the security responsibility for what he builds on the infrastructure that he rents from the cloud provider, latter must only take care of the foundational infrastructure security features.

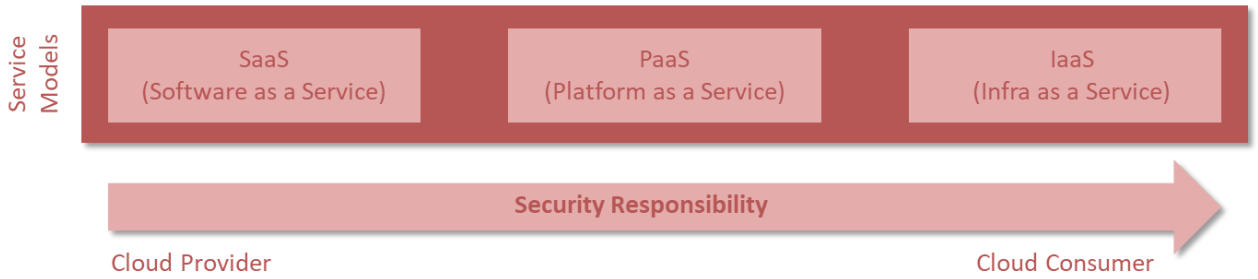

Figure 2: Shared Responsibility Model (Source: Own illustration inspired by CSA report)

A very crucial security consideration is this split of responsibility and knowing clearly which party is responsible for what. This can get quite tricky: Imagine a customer deploying multiple services in different service models from different cloud providers, the overall landscape of security responsibilities will vary and become complex. Before starting any deployment, we need to make sure to understand the security relationship between the provider and the consumer to prevent any unfilled gaps that might lead to potential security vulnerabilities. Therefore, the cloud provider must explicitly document his internal security controls and features. Based on this documentation, the cloud consumer can evaluate for every cloud project the implementation of the security and the corresponding responsibility. How can the customer be sure the provider designs and implements his controls properly? Here, the trust towards the chosen cloud service provider comes into play. In no customer-supplier setting, the customer has full control over every single process, component, and procedure behind the production (or the operation in case of a service), otherwise he would need to produce it all himself. There is a trade-off between control and trust. Cloud computing allows the customer to delegate some of the responsibilities to the provider, but towards his own clients, the cloud customer is still solely accountable for security regardless of the risk delegation. The goal is to find the most **trustworthy cloud provider**, to know the responsibility split and to implement the proper controls correctly.

RISK MANAGEMENT

Overall, risk management can be defined as the process of identifying, analyzing, prioritizing, and monitoring threats. From a business perspective, these are mainly threats to the capital and earnings of the organization and finally its reputation and existence. The risks can come from various sources, such as finance, legal, technology, nature and many more, heavily depending on the industry and business model an organization is operating in. The fact of "managing" those risks implies a proactive approach of developing strategies to mitigate the top risks and to implement controls to minimize the impact of the potential risks. Resources are usually limited, and therefore organizations must focus their resources on the mitigation of their top risks. How can you know your top risks? There is a very basic, incomplete formula to evaluate

the importance of a risk: Risk = Impact x Probability. Although it is an extremely simplified approach, it still gives a first indication of the risk importance for the considered business. Further, there are more sophisticated mathematical and statistical models that can calculate concrete monetary risk based on proven concepts. The huge amount of data we have today as well as the access to specific statistical software also allows us to run fairly accurate risk modelling and simulations based on high quality data.

Enterprise risk management is important for every organization to protect efficiently and effectively against losses and to ensure a healthy, sustainable business. Moving forward in this paper, we are only concentrating on cyber security risks for enterprises leaving all other potential risks untreated.

CYBER SECURITY RISK MANAGEMENT

Zooming out and looking at the bigger picture of where to situate cyber security risk management within an organization's governance hierarchy (see figure 3). We can put **governance** at the top of all the policies, processes and controls that are implemented within an organization. **Enterprise risk management** needs to be part of the governance and it includes the management of all relevant business risks as introduced in the previous section. It should be aligned with the predefined risk strategy, the risk appetite and risk tolerance of the specific organization. **Cyber security risk management** is one type of risk, being part of the overall enterprise risk management. It covers the management of risks related to information and technology assets that affect the confidentiality, integrity, and availability (CIA) of these assets. Furthermore, it can include improvement of the cyber security posture and ensure compliance with relevant regulations and standards. Arriving at the end of this branch of the hierarchy, we find the area of **cyber security**. Remember the statement in the introduction of this paper mentioning that security is a risk business. In this context, cyber security consists of the measures which are implemented to manage and mitigate cyber security risks. Closing the circle, we summarize as follows: Cyber security is a horizontal discipline represented in multiple areas of a company. It can for example be considered as a tool of cyber security risk management, which is part of enterprise risk management, and this is then again part of governance.

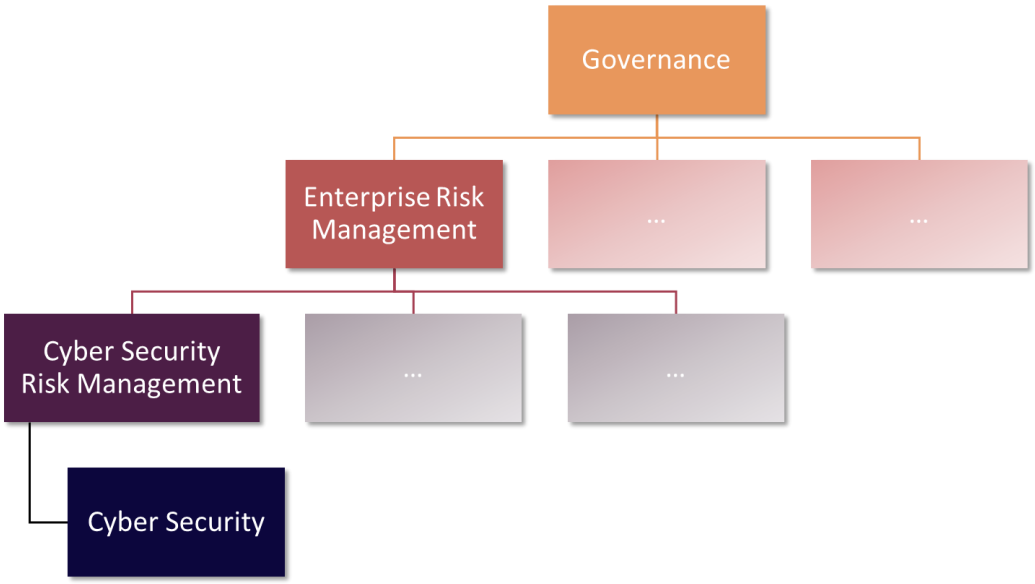

Figure 3: Cyber Security in the Enterprise Governance Hierarchy (Source: Own illustration inspired by CSA report)

Cyber security risks can come from various sources, both from external and internal exposure. As the IT environments get more complex and need to satisfy multiple needs, today's risk perimeter also gets broader. By collaborating in a digital world, with third parties, on mobile devices, from different locations and dealing with huge supply chains, the risk exposure changes as well. To mitigate these risks effectively combining technical, organizational (e.g awareness training), and physical controls (e.g locked office spaces) is a proven best practice approach. We are going to cover the main technical controls in more detail later. Cyber space and the related threats are continuously evolving. Therefore, it is crucial to regularly review the security measures in place and challenge their effectiveness regarding the current security

requirements, including potential new and emerging threats. The need for risk prioritization and faster decision making is a consequence of this change that organizations should adopt.

According to a study conducted by PwC in 2022, the four top drivers for increased cyber security risks are remote and hybrid work, accelerated cloud adoption, increased data volumes as well as convergence of IT and OT. More than 50% of the companies state they don't have the right controls in place to prevent serious cyber incidents. Moreover, with the fast-pursuing digitalization the cyber security risk might exceed the risk appetite of many organizations. Unfortunately, the probability models for traditional risk analysis are not yet accurate enough for cyber security due to the lack of data about cyber incidents, both for the likelihood and for the financial impact. Organizations cannot only rely on risk analyses, but they have to build up strong cyber resilience at the same time. In the next chapter we will introduce the concept of cyber resilience while bringing it into the context of cyber security risk management and outline some recommendations on how to approach it.

CYBER RESILIENCE

How can we adapt to rapid, disruptive changes and emerge from them even stronger? The solution is called "resilience". As important personal resilience - the ability to withdraw and recover quickly from difficulties - is for every human being to master challenging situations in live, as important cyber resilience is for companies to bounce back from cyber attacks and to keep up with today's cyber challenges. The National Institute of Standards and Technology (NIST) defines cyber resilience as follows: "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." The concept of cyber resilience requires to be able to adapt constantly and spontaneously to unexpected situations which is very much related to human life. To ensure competitiveness today, we need to be agile, flexible, innovative, disruptive but especially resilient.

What is the difference between cyber security and cyber resilience? Cyber security covers the methods and procedures to protect data and IT systems using mostly technologies and business processes. Whereas cyber resilience is the ability to recover from a cyber incident that occurred. Both are equally important and strategic. The development of an effective cyber security and cyber resilience strategy is an ongoing task because cyber threats are constantly evolving.

Better start today than tomorrow, and it is never too late to start becoming cyber resilient. You could for example start by making your board of directors aware of the importance of cyber security and cyber resilience. It is also recommended to implement a cyber incident response plan, simulate a security incident with your company and implement basic security hygiene with security fundamentals - just to name a few recommendations.

FAMEWORKS FOR CYBER SECURITY RISK MANAGEMENT

With new types of cyber attacks and a continuously growing digitalization of all business areas, there also comes an increasing complexity of cyber risk management. Executives are aware of the challenge, and they ask for full transparency around cyber risks. Their goal is to find the right ways to manage the risks actively and protect their organization. Unfortunately, an effective and integrated, holistic approach to cyber security risk management is often missing. For the board members easy to interpret reporting based on a reliable data source is key. But organizations often struggle with lack of structure (too many KPIs and poor quality), lack of clarity (a lot of acronyms and technical terms) and lack of consistent real-time data (one single source of real-time data missing).
There are several well established frameworks that can be used as guidance. They provide a proven set of best practices and guidelines which can be followed to evaluate potential risks and decide how they will be mitigated. Probably two of the best-known frameworks are the NIST Cybersecurity Framework and the NIST Risk Management Framework, including valuable guidelines for managing security risks in the public cloud. Further frameworks can be found from the International Organization for Standardization (ISO), specifically the ISO 27001, and the one from the Cloud Security Alliance (CSA). These resources are mostly available for free and can be accessed easily.

When taking a holistic cyber risk management approach (see figure 4), an organization has its most valuable **data** in the center of the attention and builds a layered protection around it. First, the inventory of critical **assets** is important to know what has to be protected and where. Then, well-chosen **controls** are put in place with the goal of balancing security with agility - hindering the business unnecessarily would be counterproductive. The next layer consists of proven best practice

security **processes** focusing on effective response. Cyber security needs to be part of the **organization**'s culture. Furthermore, the right skills, efficient decision making and cross-functional enterprise-wide cooperation are additional success factors. The last layer is represented by the **governance**, laying the foundation for the investment in cyber resilience and transparency into cyber risks. With this approach, the organization is empowered to focus their resources on the most likely and most threatening cyber security risks. The highest controls are applied to the most crucial assets, thus allowing to achieve a balance between effective cyber resilience and efficient operations.

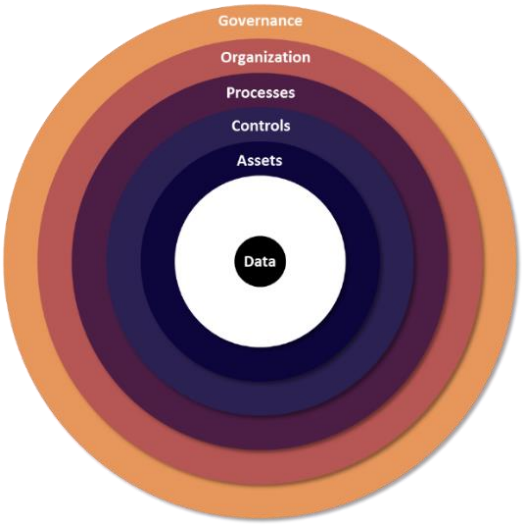

Figure 4: Holistic Cyber Risk Management Approach (Source: Own illustration inspired by McKinsey)

In order to find out how to mitigate top risks, a four-step path (see figure 5) can be followed. **First**, a list of critical assets, known risks and potential new risks will be elaborated. Based on this list, the upper management decides about the risk appetite and the prioritization of the identified risks. This is a highly critical and important step which can have big existential consequences for the company. Therefore, the board is involved and has to take the ownership and final decision. **Second**, the likelihood of occurrence and the potential impact of the previously defined risks is evaluated with regards to operational, financial, regulatory, and reputational impact. **Third**, an overview of all initiatives that are undertaken to mitigate the top cyber risk is created. With the implemented initiatives, the residual risk should then fall within the parameters of the organization's risk appetite. **Fourth**, keep the management updated about the treatment and remediation of the top risks using an easy to interpret monitoring system or dashboard. It should be understandable for a board member without special cyber security know-how, avoiding acronyms and technical jargon. And there we go again, restart with the first step because cyber security risk management is a continuous process.

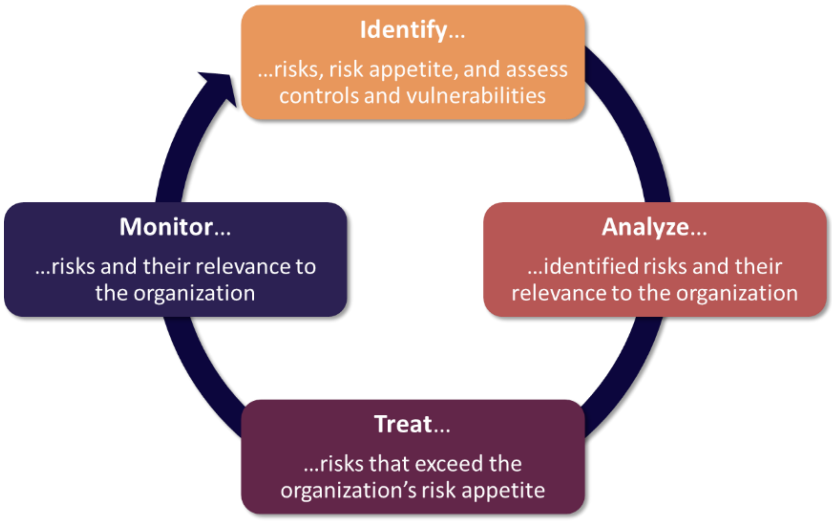

Figure 5: Risk Mitigation Path (Source: Own illustration inspired by McKinsey)

CYBER SECURITY IN THE PUBLIC CLOUD

We are now getting to the tricky question about the impact on cyber security when moving from an on-premises infrastructure to the public cloud. Let's introduce and consider some important aspects regarding cyber security in the public cloud. As we have learnt, in a public cloud deployment model the cloud provider is responsible at least for the management and operation of the infrastructure and normally there is very limited room for customization of contracts. The scalability of the public cloud lives from the characteristic of economies of scale through resource pooling and the property of multitenancy (multiple customer tenants using the same infrastructure). An easy comparison: You are the tenant of an apartment in a house. For all the tenants of this house, the heating system will be the same, there is no room for individual adjustments. Therefore, public cloud contracts are inflexible. Examples of public cloud providers include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. The main responsibility of the providers is to ensure service availability, accessibility, and compliance of their service.

The fact of moving from a traditional mostly on-premises infrastructure to the public cloud doesn't change the risk tolerance of a company, it only changes the way these risks are managed and by whom. It might come along with new risks and make some traditional risks less relevant. I would like to outline some of the major cyber security areas being relevant in a public cloud environment and how they can be handled (see figure 6).

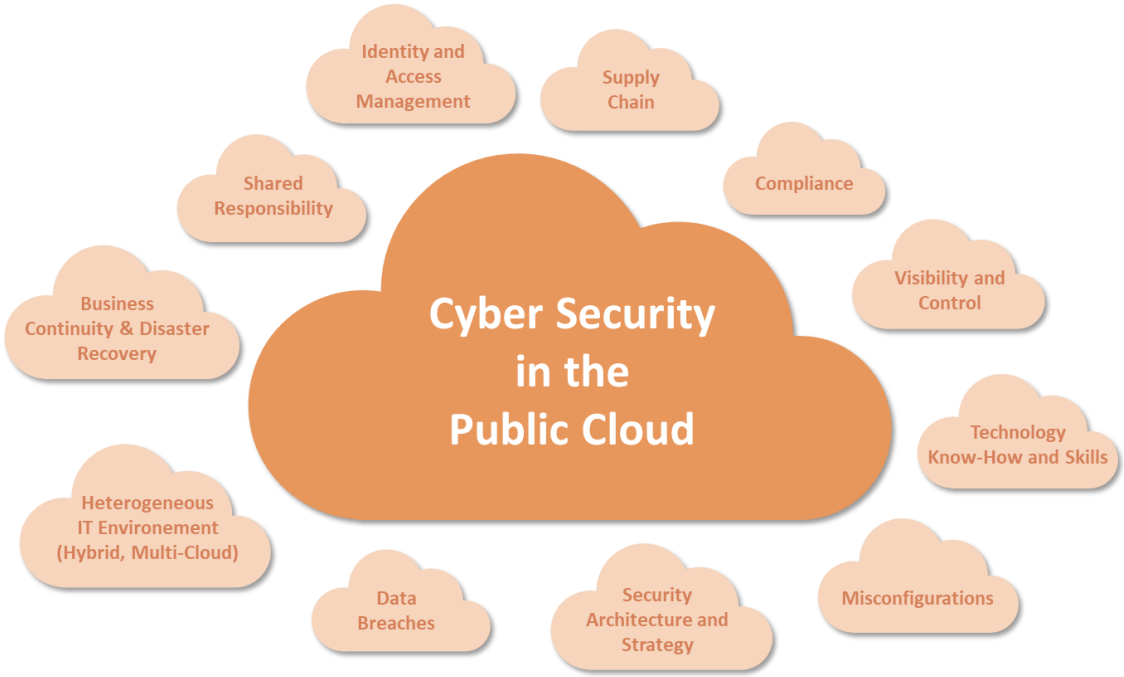

Figure 6: Cyber Security in the Public Cloud (Source: Own illustration)

- **Security Architecture and Strategy**

A lot of companies jump to the cloud without being properly prepared. A move to the cloud needs thorough preparation, a strategy and a carefully thought-out security architecture aligned with the new environment. It is highly recommended to ensure that the security architecture aligns with the business objectives and that continuous security monitoring procedures are implemented to keep track of these goals. To do so, companies must understand how the threat landscape changes, who the adversaries are and how they behave. This allows us to adapt the strategy accordingly and become more secure and resilient. As introduced in the last chapter, organizations can leverage security frameworks to adapt and adopt established standards, best practices, and regulations. A customization of the chosen framework might be needed, especially for companies with a particularly complex and individual operation technology (OT) environment. Specific requirements need to be incorporated into the architecture. Furthermore, security and risk management practices should be top of mind everywhere, from planning, designing, constructing, and operating projects. The "secure by design" approach is a critical component of a future-proof security strategy.

- **Supply Chain**

Supply chains often get more complex when moving to the public cloud. You typically have more interfaces with different external stakeholders, and you must rely on services and products you get from third parties. The threat of supply chain attacks and thus the importance of supply chain security increases because there is a loss of control and a higher dependency on suppliers. When choosing a supplier, especially when choosing a cloud service provider, it is necessary to investigate the security and compliance measures of the named company, review and assess them. If the supplier or provider himself outsources parts of his services, be aware of the third parties and how they might affect your security posture. Through contracts and service agreements you can agree with suppliers on concrete aspects but don't rely too much on contracts. Enhanced visibility, transparency, communication, and collaboration with suppliers as well as balancing the security and trust can help mitigate the risk of security vulnerabilities along the supply chain.

- **Heterogeneous IT Environment (Hybrid, Multi-Cloud)**

When the IT environment becomes more heterogeneous with different service and deployment models from multiple providers, the complexity rises. "Complexity is the biggest enemy of security" – that's what we learnt during the first class of the course "Introduction to Information Security". Managing multiple environments requires to coordinate more resources internally and externally. With each vendor you will have a different relationship, contracts, and service offerings. In some cases, it can make sense to adopt a multi-cloud strategy, using several cloud providers, rather than relying on one single provider. It allows for example to take advantage of different capabilities, pricing models and data redundancy. But as stated, the downside is increased complexity which can lead to a security risk if not managed properly.

- **Shared Responsibility**

We already covered this concept (page 3), which is an important aspect of cyber security in the public cloud. The shared responsibility model has an impact on the overall security strategy and architecture. The responsibilities should be documented, and the boarders clearly stated to make sure no security gaps are left open on the boarders of responsibility between the cloud provider and the customer. Understand what responsibilities you have as the customer and what the cloud provider is responsible for. Based on this you can implement the necessary security controls in line with the risk appetite and strategy of your company.

- **Business Continuity & Disaster Recovery**

Business continuity (BC) and disaster recovery (DR) are important mechanisms allowing organizations to keep their business up and running during an outage caused by an unfortunate and unpredictable event (security incident, natural catastrophe etc.) and to avoid operational downtime. The same as for an on-premises infrastructure, BC and DR are important topics for public cloud computing. It is also part of the shared responsibility model because some aspects are managed by the cloud provider and some by the customer. For organizations with traditional IT environments not having a modern BC and CR in place, migrating to the cloud can be seen as an opportunity to use the cloud capacity to improve regarding this area. Data backups in the cloud, stored in an off-site location, can for example be a benefit if the own data center is affected. A lot of cloud providers offer additional functionalities that customers can implement for BC and DR in the cloud and there are many automation techniques to support. Before you invest a lot of money, know the processes and assets of your company. You then also know the business-critical parts where continuity and recovery are crucial. Make sure you have waterproof BC and DC strategy for the processes and assets that need perfect availability. For the other, less critical areas, you might accept a certain downtime in case of an emergency.

- **Visibility and Control**

Visibility and control are still a concern that is often raised by IT admins when considering moving to the public cloud. While transitioning to the public cloud, customers lose some visibility and control because they rely on the operations of the chosen cloud service provider. There are mainly two challenges regarding visibility and control in the public cloud. First, the risk of shadow IT, meaning that employees use applications not approved by the internal IT. Second, the misuse of IT-approved applications, leading to potential data loss and breaches. Both can be managed using tools such as Cloud Access Security Broker (CASB), that will be introduced in the next chapter. Besides the implementation of technologies, user awareness is also an important point in this case. Companywide training for cloud usage and how to deal with the use of applications can help to make the employees aware of their responsibility regarding compliance and security in the public cloud.

- **Technology Know-how and Skills**

"Every company is an IT company" we often hear. Today, building cloud-based solutions and business applications is not only possible for tech-companies anymore, but every organization aims to have their own team to generate custom digital products and services, instead of relying on third-party vendors. This shift leads to two big challenges. On the one hand companies don't have the know-how and skills in-house yet, so they are looking for cloud workforce on the market. On the other hand, good cloud computing experience and knowledge is a very rare skill on the labor market. These two facts combined make cloud computing one of the most sought-after skills nowadays, regardless the industry and geography. Organizations can for example overcome the skill shortage by investing in their own workforce, reallocating existing talents and reskilling motivated employees. There is a huge offer of training possibilities that can be accessed if you are willing to invest in the lifelong learning of your staff. Additionally, the revision of hiring processes and salaries will also play an important role in acquiring new cloud experts. Without having the right skills and know-how available for your company, your cloud security posture might suffer.

- **Misconfigurations**

Having mentioned the challenge of skilled cloud experts, the risk of misconfiguration is quite obvious when implementing a service you are not familiar with. Although you might have a lot of tools available from the cloud service provider, it remains the customer's responsibility to configure and implement the technology correctly on his side. Misconfigurations can lead to vulnerabilities and increase the risk for a company of being compromised. For example, insecure storage and excessive permissions are misconfiguration that are often seen, and they can be inhibited or detected automatically by technical measures, which will be explained in the next chapter. Besides upskilling your staff or hiring cloud-savvy people, here again, user awareness is essential. It is also recommended to conduct security assessments regularly and to have a strong incident response plan in place.

- **Compliance**

Compliance standards vary a lot depending on the industry and company. The good point with cloud computing is that here as well, the service provider has his responsibility stack. The service you consume (providers responsibility) needs to be in line with your compliance requirements and the way you use (customers responsibility) them as well. Usually, cloud providers have compliance certifications you can access and review before signing a contract. But if the implemented standards and regulations don't follow your own requirements, there will be almost no room for customization of the contract, and you should probably look for a more suitable supplier. Ensuring compliance with your internal regulations, industry standards and the official law gets even harder if you are running a multi-cloud environment because it requires the management of multiple vendors. Thanks to the evolving technology and innovative processes a huge part of the monitoring of compliance can be automated today.

- **Data Breaches**

The loss of data is considered as one of the top cloud security threats. It brings together some of the points we have covered earlier in this section that can obviously lead to data breaches if not implemented correctly. It is closely related to reputational, regulatory, and legal risks. With new data privacy regulations (e.g. GDPR, SDG), this point becomes even more important. We can benefit from several mechanisms that can be put in place to prevent such data breaches, going from technical measures such as encryption, to the principle of least privilege and enhancing user awareness.

- **Identity and Access Management**

Identity and access management (IAM) is another hot topic when talking about cloud security threats, or cybersecurity in general. Public cloud platforms are typically well accessible making it possible to access them by the internet from almost everywhere. This comes with a lot of benefits but also brings along some new security risks. Organizations might struggle to manage the ever-growing inventory of identities and accounts in the cloud. Therefore, it is indispensable to implement strong access controls and prevent unauthorized use of confidential resources. For example, using multifactor authentication and implementing strict access control can already tremendously reduce the security risks related to IAM.

MITIGATION OF CYBER SECURITY RISKS IN THE PUBLIC CLOUD

Already today, there are a lot of tools and mechanisms available to mitigate cyber security risks in the public cloud and to address the challenges we covered in the last chapter. In this chapter some of the most important existing mitigation areas will be introduced and future trends will be discussed.

MECHANISMS AND TOOLS

We can structure the main mechanisms and tools for risk mitigation in the public cloud alongside the five phases of the well-known NIST cybersecurity framework (see figure 7). The first phase **Identify** has the goal of understanding the organization's critical processes, the asset inventory, and the related top risks. The following phase then focuses on how to **Protect** the previously defined assets. Although it is good to protect, companies should adopt a so called "zero trust" mentality, meaning that you don't rely only on protection mechanisms, but you always look out for a potential intrusion, and you try to verify everything. To do so, you need to be able to efficiently **Detect** unusual activities or anomalies. In case you detect an incident, you should have the needed capabilities to **Respond** quickly. Once resolved you ideally have the right tools in place to **Recover** from the incident. This is just to briefly introduce the process of the framework and put it into the context of this paper. The entire framework is available on the NIST website for more detailed study.

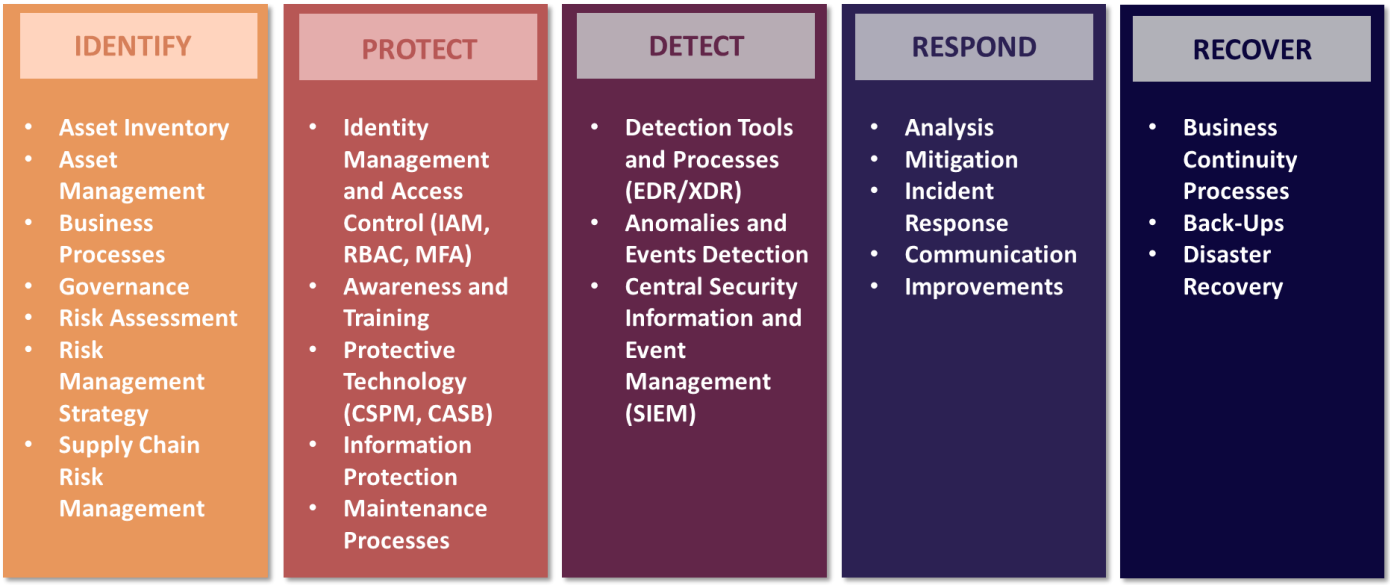

Figure 7: Cyber Security Mechanisms and Tools (Source: Own illustration inspired by NIST)

- **Identify**

The goal is to gain a better understanding of the IT environment and identify exactly which assets are at risk. A lot of organizations struggle with the visibility on their assets, but a thorough asset inventory lays the foundation for all the following phases. You first need to know what you own and what you want to protect. Asset management is about managing the data, personnel, devices, and systems aligned with the organization's risk strategy. Transparency and visibility on the critical business processes is an additional point which needs to be worked out in this phase. A central cloud identity provider can for example help to identify and manage key assets (user identities, devices, apps, etc.) while enabling functionalities such as single-sign-on and mobile device management. Based on the asset inventory and the business processes overview, an appropriate overall risk management strategy as well as supply chain risk management strategy can be elaborated.

- **Protect**

The tools and mechanisms in this area focus on policies and procedures to protect the IT environment from a potential cyber security attack or unvoluntary data leakage. Cloud based identity and access management (IAM) tools can help to control access to the resources, including authentication and authorization measures, such as multifactor authentication (MFA) and role-based access control (RBAC). Some cloud providers for example offer with their cloud identity solutions integrated possibilities for conditional access policies. Based on preconfigured conditions (user, device, application, location, risk etc.) an organization can set the right level of access control. In addition to these automated mechanisms,

profound and recurring user awareness training is key. According to various studies (e.g. IBM, PwC, Microsoft), more than 90% of today's cyber security breaches result from human error. If we can train employees in how to handle data, documents, systems, and processes in a secure way, this can already have a significant positive impact on the protection.

There are further protective technologies available in the cloud, such as the cloud access security broker (CASB) which provides a check point between the user and the cloud application. It enforces the data security policies established by the organization and allows to integrate the needed controls for legitimate access of the applications. Another well-established protection mechanism is called cloud security posture management (CSPM). It looks for misconfigurations across the IT infrastructure of the company and gives visibility into the overall security posture. Additionally, firewalls on networks, host and applications are configured with the needed policies to block unauthorized and malicious traffic. Moreover, a crucial information protection mechanism is provided through encryption. Encryption tools can ensure the confidentiality and integrity of information while storing, transmitting, and using them in the public cloud.
The importance of maintenance should not be underestimated. Products and services are continuously evolving, and vendors are updating them with new features. An important part of these improvements is designated to security. Therefore, it is highly recommended to maintain the systems and to always keep them up to date with the latest version and security features.

- **Detect**

It is good to be well-protected against cyber attacks but if you adopt the concept of "assume breach" this makes you even more secure. By assuming that you have been compromised, you look out for breaches, and you try to detect anomalies as soon as possible. To facilitate the detection of such anomalies and security breaches, there are specific systems and procedures available. Cloud providers offer advanced security solutions for threat protection in real time. So called endpoint detection and response (EDR) or extended detection and response (XDR) tools provide the necessary protection as well as threat detection, investigation, and response by using threat intelligence and data analytics to better automate security operations. Furthermore, centralized security information and event management (SIEM) tools help to monitor the whole IT environment by collecting and analyzing security-related data from multiple sources. Such detection systems can provide valuable visibility into the security posture of an organization and help to foster it.

- **Respond**

If a cyber incident occurs, it is very beneficial to have the tools and procedures in place to react efficiently and effectively to the attack. Some of today's extended detection and response (XDR) tools can not only detect but also automatically respond to an attack. They provide reports and analyses consisting of valuable insights into what's going on within the IT environment. Incident response planning on a technical but also on an organizational level is highly recommended. Communication paths and responsibilities should be defined and trained upfront, in case of an emergency it's only about execution and no time should be lost. While testing your response capabilities, you see where some improvements can be made and how you can become more efficient and effective in a real-case scenario.

- **Recover**

In case a company is compromised, the main business processes should be kept up and running while the incident is being treated and resolved. To do so, solid business continuity processes need to be prepared upfront to assure the critical business can continue even in case of a cyber attack. In parallel, data back-ups will help to recover from a potential loss of data. Copies of data can for example be maintained separately in a cloud backup and will not be affected from an attack on the specific network or servers. This can ensure quick disaster recovery when the original data is not available anymore.

As we can see, there are a lot of security tools and mechanisms available which are state of the art when it comes to mitigation cyber security risk in the public cloud. Organizations only need to acquire and implement them correctly. Due to the lack of security resources, the increased automation of security analysis and mitigation is very helpful. More sophisticated technologies can permit us to fill a part of this skill gap. It remains important to regularly review and update these tools and mechanisms to ensure they are effective in addressing emerging threats and mapping the evolving security requirements.

FUTURE TRENDS

We learnt about the commonly available security tools being in use today, let's now go a step further and have a look at the future trends in cloud security. According to Gartner, an international IT research firm, cloud-based security products are the fastest growing market segment in IT security. The recent version of the Gartner Hype Cycle for Cloud Security (see figure 8) shows the most significant technologies in this area. Gartner uses the hype cycle as a graphical representation for the maturity, adoption, and application of emerging technologies through the timeline of five phases. The curve shows the general market expectation for the products in each phase of the cycle and gives an indication of the speed a certain technology is moving forward in its adoption journey.

The cycle starts with the **innovation trigger** which is kicked off by a breakthrough, a public demonstration, or an event generating press and industry interest in a certain technology. From there, the expectations of the capabilities the innovation will bring are rising fast up to the **peak of inflated expectation**, where we imagine it to be capable of results that are not reality (yet). The impatience and lack of concrete results of the technology will then lead to the **trough of disillusionment**, literally we feel disillusioned with the technology because it doesn't hold what it promised. Some ambitious people will continue believing in this specific innovation and try to make it work. Once they can prove it, they enlighten others, and they will be followed. This phase is called the **slope of enlightenment**. Finally, the **plateau of productivity** will be reached once a lot of organizations feel comfortable using the technology and it is going to be widely adopted.

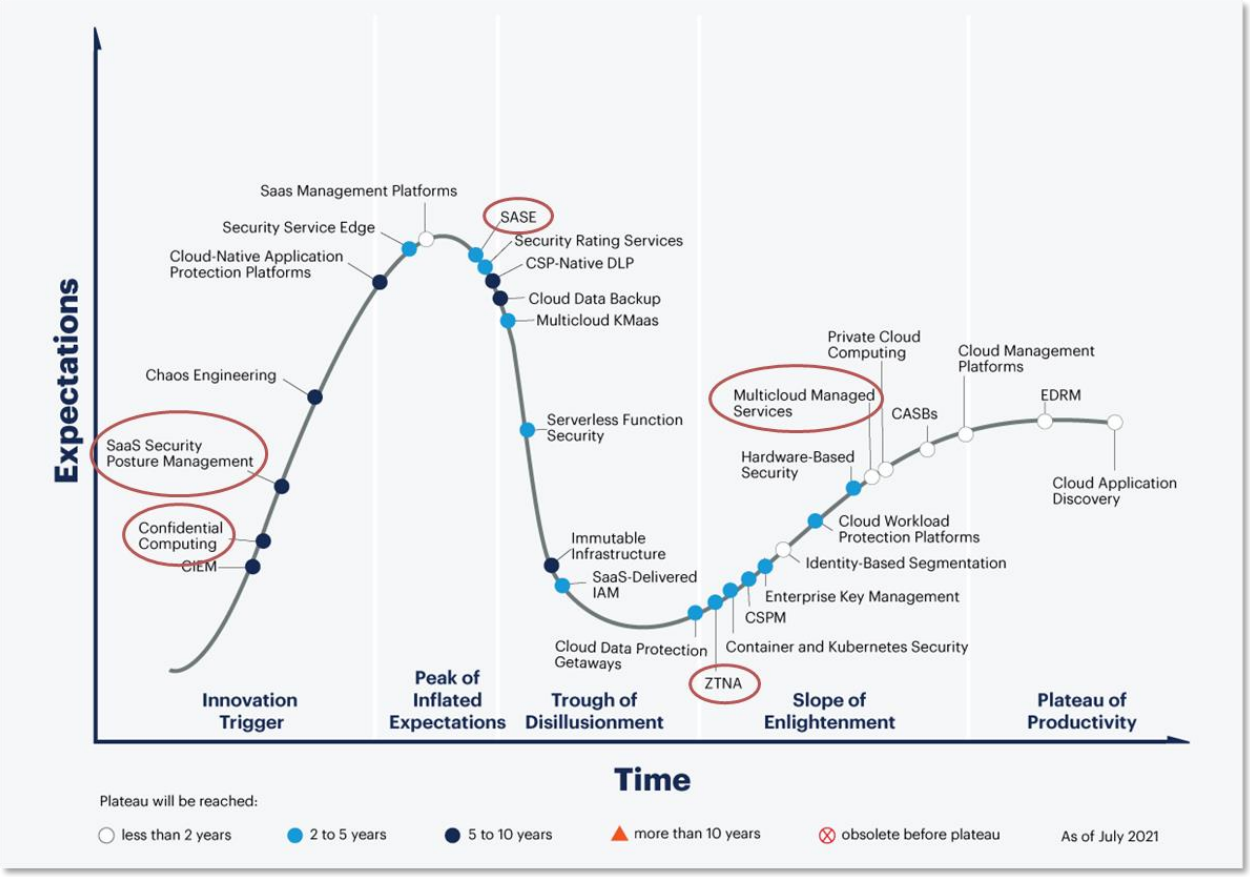

Figure 8: Hype Cycle for Cloud Security (Source: Gartner, 2021)

Looking at the hype cycle, we can find some of the tools we already introduced in the previous chapter as they are widely used today, such as CSPM and CASB. According to Gartner and other industry experts, several of these technologies might become less important or even obsolete in the coming years, such as private cloud computing (lack of scaling) and cloud data protection gateways (not suited for cloud services). Others are more promising, and they are predicted to enhance cloud security significantly. Let's highlight some of the most important innovations.

- **Confidential Computing**

Considering a situation where we are in an extreme attacker model with a malicious operating system. In such a case, confidential computing can protect data in so-called trusted execution environments (TEE). A TEE is an environment on the hardware providing a protection of data in use. Such systems are available from different hardware vendors, and they can solve many existing problems (e.g. prevent use of malware, data breaches). Even though this innovation is currently still in the phase of innovation trigger when looking at the hype cycle, it seems to be very promising due to the fast-evolving threat models.

- **SaaS Security Posture Management (SSPM)**

SSPM is an evolution of the cloud security posture management (CSPM) we have seen in the previous chapter. Basically, it does the same with a focus on SaaS applications. The tool continuously assesses the security risk and manages the security posture of a company's SaaS application landscape. Core capabilities include reporting the configuration of native SaaS security settings, managing identity permissions, and offering suggestions for improved configuration to reduce risk. Most organizations use hundreds of SaaS applications, and with cloud adoption the number of applications is growing even more in the coming years. SSPM tools reduce risk by continuously scanning for and eliminating configuration mistakes, which are the most common cloud security failures. Looking at the hype cycle, we can find SSPM still in the phase of innovation trigger but CSPM - his older brother - is already on the slope of enlightenment. SSPM will probably be there in approximately five years as well.

- **Secure Access Service Edge (SASE)**

SASE is delivered as a service by cloud providers and enables access to systems based on the real-time identity of a device or entity, combined with security and compliance policies. SASE significantly simplifies the delivery and operation of critical network security services mainly via a cloud-delivered model, increasing agility, resilience, and security. Although this technology might be adopted by a large number of organizations in the coming years, there is also a need for new models looking beyond the network perimeter. Some ideas go into the direction of the "zero trust" and an identity-based approach.

- **Zero Trust Network Access (ZTNA)**

ZTNA is a security solution that enables secure access to an organization's internal application, data, and services for remote users. As the name states, it is based on a "zero trust" model, meaning that trust is never implicitly given. Access is only granted on a least-privileged basis by clearly and granularly defined control policies. Thus, it allows secure connectivity to apps without exposing them to the network and the internet. Most likely, this technology will be widely adopted within the next five years.

- **Multi-cloud Managed Services (MMS)**

MMS allows software-based management of a multi-cloud environment. Businesses - especially large companies - will use cloud services from multiple cloud service providers at the same time which makes its management more complex. Thanks to MMS, the governance and lifecycle management of all the different cloud resources can be automated.

F I N D I N G S

In this section, I will reflect about the overall content while presenting my personal thoughts. Some of them are closely related to other topics we have covered within the lectures of "Contemporary Topics in Cyber Security" and some others are more connected to my professional role and my everyday work life.
Before reading my critical view, hold on a minute and think about your own point of view. What do you think about the topic discussed in this paper? If you feel like sharing it with me, please do so. I'm always interested in widening my horizon and learning about other perspectives.

CRITICAL VIEW

I want to stress some points that came to my mind while working out this paper and they might be a whole area of reflection and elaboration by themselves.

- **Public cloud versus on-premises**

Since I started working in IT six years ago with a specialization in cloud computing, I find myself in between two statements. On the one hand, cloud providers saying that moving to the public cloud makes the customer's IT environment more secure. On the other hand, customers worrying that moving to the public cloud makes their IT environment less secure. Two contradictory statements, but which one is correct? I would say: It depends... If an organization moves to the public cloud without being aware of the responsibility boundaries between the cloud provider and himself, not having the needed knowhow and skills, without providing user training nor implementing any specific security solution, in this case it might probably make the concerned organization less secure and more prone to cyber security incidents. In contrary, if an organization moves to the public cloud well-prepared, knowing what their own and what the provider's security responsibilities are and how to control them, having cloud-savvy employees inhouse, fostering user awareness and implementing the security tools and mechanisms available to identify, protect, detect, respond, and recover, this organization will enhance its security posture comparing to staying on-premises.

- **Best-of-suite versus best-of-breed**

We know the principle of "the winner takes it all". Is this also going to happen with cyber security solutions in the public cloud? Are the big cloud providers (Amazon, Microsoft, Google) taking it all? What we have seen during the last years is the following: Multiple start-ups and passionate professionals solve a narrow problem and once it is proven to hold what it promises, the start-up is acquired by a large player. The big companies usually don't build the solution in-house but acquire the innovation in an early stage to then develop and adapt it to their suite of products. Looking at the big cloud providers, they bet on the strategy of a cloud platform and therefore a "best-of-suite" approach. Whereas small, very specialized security vendors try to survive with their niche product, and they promote the "best-of-breed" approach, meaning that customers should always chose the best solution for every security need instead of putting all eggs into the basket of a single cloud provider. This game between point-solutions (best-of-breed) and platforms (best-of-suite) is not decided yet, but so far, the trend is going into the direction of the cloud platform providers. It allows customers to reduce complexity, number of suppliers and security costs all at once. We see this trend confirmed by the fact that Microsoft has been the largest cyber security company in terms of annual revenue in 2022 and their ambition is to constantly grow. For sure there is always a trade-off between the reliance on one vendor and splitting it off to multiple vendors reducing the dependency on each of them. We have seen that both options come with different security risks. I personally think that choosing one trustworthy public cloud provider is fine for small and middle-sized companies, but for large enterprise customers it might make sense to have a multi-cloud strategy.

- **Impact of quantum computing, machine learning and artificial intelligence on cyber security risks**

As for every new technology, it can and will always be used for good and for bad. In the course "Introduction to Information Security" we have discussed the potential impact of quantum computing can have on security mechanisms, namely encryption alogrithms. Some of the algorithms considered secure in the presence of normal computers may not be secure anymore in the presence of quantum computers. What will be its impact on the cyber risk landscape and the management of cyber security risks for an organization?

Similarly for artificial intelligence (AI) and machine learning (ML), both will considerably improve today's cloud security services by recognizing patterns, uninteded behaviors and threats even faster. But such technologies can also be used in a bad intent. The famous chatbot "ChatGPT" based on AI, for example, can be useful to answer basic questions and to build knowledge. However, he can also be abused for cyber attacks, namely by writing phishing e-mails and code for malware.

- **Impact of geopolitical situations on cyber security risks**

Cyber space is not the only dimension of this world. There is also the physical space and maybe even other "spaces" having an impact on cyber security. To take the recent example of the Ukraine war, we recognize an obvious impact of the war on the cyber risk for all uf us. Cyber attacks between the fighting countries can easily spread all over the world within a very short time. In this unpredictable time, it is even more important for organizations to be ready to react and to be cyber resilient. The impact of geopolitics on cyber security risks is not to be underestimated and might become even more important in the future.

CONCLUSION

(ZERO) TRUST

- CHOOSING A TRUSTWORTHY CLOUD SERVICE PROVIDER
- ALWAYS VERIFY, BE PREPARED TO DETECT AND RESPOND

RESPONSIBILITY

- KNOWING EVERYONE'S RESPONSIBILITIES AND THEIR LIMITS
- TAKING OWNERSHIP AND STARTING TODAY BETTER THAN TOMORROW

CYBER RESILIENCE

- BUILDING UP CYBER RESILIENCE IS INDISPENSABLE
- ADOPTING: "THE ONLY CONSTANT IN CYBER IS CHANGE - BE RESILIENT!"

We asked ourselves a couple of questions at the beginning of this paper and I hope you got some answers to them. In summary we can point out three main areas:

- First, the importance of balancing trust in a trustworthy cloud service provider and keeping control over your IT environment. We also learnt about the concept of "zero trust" and the implying attitude to verify everything. Choosing a multi-cloud strategy should be done carefully, considering the complexity it brings. Nevertheless, it might be adopted more often in the future and emerging technologies may assist in its management.

- Second, when using public cloud services, the issue of security responsibilities between the provider and the consumer is highly relevant. Depending on the service and the deployment model chosen by the customer, responsibilities are divided differently. Both parties must take ownership of their security obligations, put the needed controls, mechanisms, and tools in place without creating a security gap between their responsibilities.

- Third, we questioned the purely risk-based approach of cyber security given its unpredictable, disruptive, and ever-changing landscape. Building up cyber resilience seems to be indispensable for organizations to survive in today's cyber space. The combination of a well-thought-out security strategy with the implementation of proven tools and mechanisms is considered a best practice. It is also important to think about the human factor and raise user awareness. By far the most essential learning of this paper is to remain vigilant, adopt a mindset of constant change and stay aware of emerging trends in both protective mechanisms and threat models.

We have seen that the topic of managing security risks in the public cloud can be extended to multiple other areas, such as quantum computing and geopolitical situations. Further research is required to dive deeper into these areas. The list is for sure not complete, additional considerations may be thought of when it comes to the complexity of cyber security risk management today. This makes the subject even more interesting.

In conclusion, this paper has treated the omnipresent trend of moving to public cloud computing and its impact on organizations' cyber security risk management. We have introduced valuable insights and strategies that can help guide us towards a better mitigation of those risks. But this is just the beginning of the journey. The question now arises: What are we going do with this knowledge? Are we accepting the cyber challenges and starting to take appropriate actions or are we leaving the outcome in the hands of the opponent? The choice is ours.

SOURCES

REPORTS AND BOOKS

- Cloud Security Alliance (CSA), Security Guidance For Critical Areas of Focus in Cloud Computing v.4.0, 2021
- Cisco, Security Outcomes Report Volume 3, Achieving Security Resilience, 2022
- S. Cornovale & S. Yeniyurt, Cyber Security and Supply Chain Management: Risks, Challenges, and Solutions, 2021
- Gartner, Cloud Strategy Leadership, Gartner Insights on How and Why Leaders Must Implement Cloud Computing, 2017
- Gartner, Cybersecurity and IT Risk Primer for 2022, 2022
- Gartner, Hype Cycle for Cloud Security, 2021
- Maier S., Geschäftsrisiko Cyber Security, 2020
- Maillart T., Doctoral Thesis ETHZ, Mechanisms of Internet evolution & cyber risk, 2011
- McKinsey & Company, Cyber risk measurement and the holistic cybersecurity approach, 2018
- NIST, Cloud Computing Security Foundations and Challenges, based on different NIST publications, 2017
- PwC, 2023 Global Digital Trust Insights, The C-suite playbook on cybersecurity and privacy, 2022
- PwC, Vulnerability Management, Why managing software vulnerabilities is business critical - and how to do it efficiently and effectively, 2022
- Schaller P., Cyber Security Outlook 2022, 2022

WEBSITES

All the following sources have been accessed between 29.12.22 and 18.01.23

- 10 Security Risk Management Habits to Adopt | Accenture
- Cyber Resilience vs. Cybersecurity: What's the difference? (bitsight.com)
- Business Continuity and Disaster Recovery in the Cloud | CSA (cloudsecurityalliance.org)
- Six Ways to Tackle the Cloud Skills Shortage | Deloitte US
- 5 Steps to Strengthening Cyber Resilience (darkreading.com)
- 12 Risks, Threats, & Vulnerabilities in Moving to the Cloud (cmu.edu)
- Here's How To Plan And Budget For 2023 Cybersecurity Trends - Forrester
- Stay Updated On Cybersecurity Trends With Our Security And Risk Service (forrester.com)
- 4 Technologien vom Hype Cycle für Cloud-Sicherheit | Gartner
- What Is Cybersecurity? | Gartner
- What is cyber resilience? | IBM
- Cloud storage vs. on-premises servers: 9 things to keep in mind (microsoft.com)
- Public Cloud vs Private Cloud vs Hybrid Cloud | Microsoft Azure
- Microsoft 365 & Security for Partners
- Azure Security Stack vs. NIST Cybersecurity Framework | Managed Sentinel
- The future of risk management in the digital era | McKinsey
- The approach to risk-based cybersecurity | McKinsey
- Perspectives on model risk management of cybersecurity solutions in banking | McKinsey
- Cloud computing transformation in banking risk | McKinsey
- What is cloud computing: Its uses and benefits | McKinsey
- Cybersecurity Framework | NIST
- Top 6 Cloud Security Threats and How to Mitigate Them (netwrix.com)
- Security and Risk Management in Cloud Computing With Examples (ostridelabs.com)
- Cyber Security Training | SANS Courses, Certifications & Research
- ChatGPT-Written Malware - Schneier on Security
- NIST Cybersecurity Framework Components Explained (swisscyberinstitute.com)
- Top 11 cloud security challenges and how to combat them | TechTarget
- Game of Thrones in cybersecurity: data gravity, industry consolidation, platform play, private equity, and the great cyber gold rush (ventureinsecurity.net)
- Risk Management for Cloud Migration - WSJ