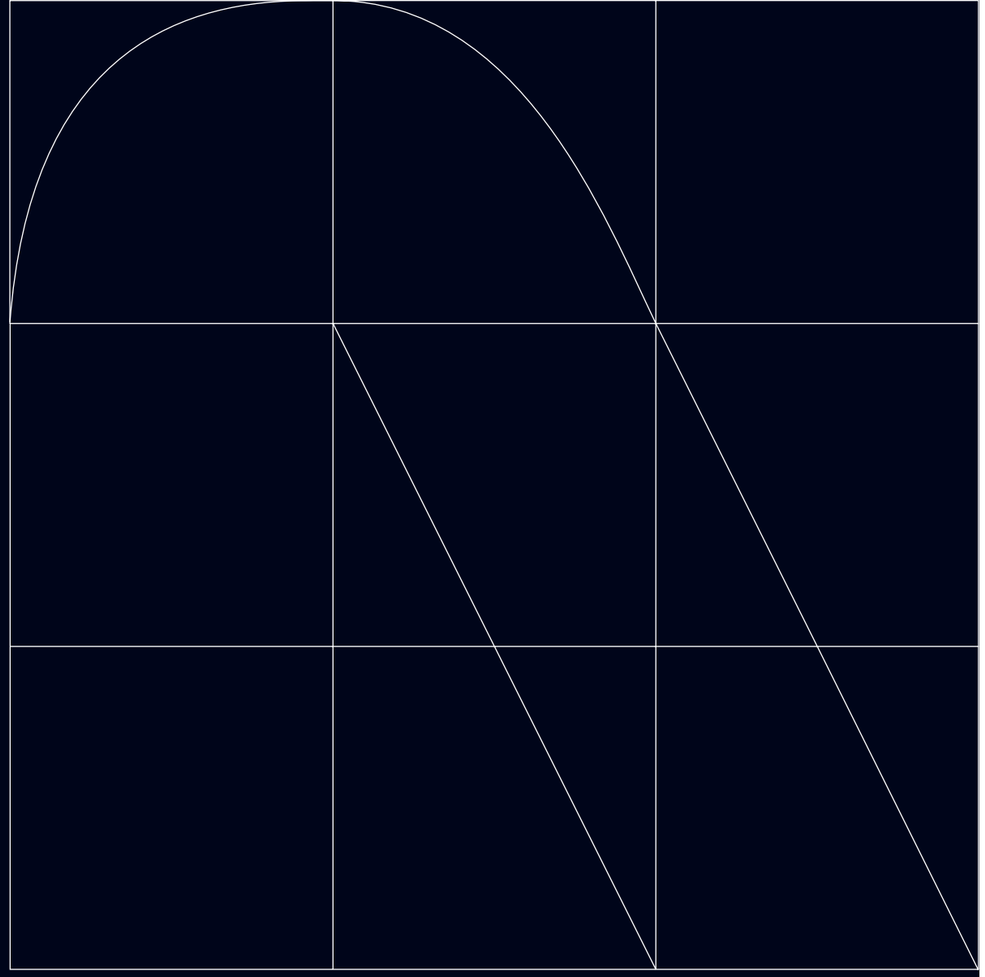
Enhancing Security in the era of Smart, Data-driven Insurance

The Challenges of Cybersecurity

Thought Leadership

Contents



Overview

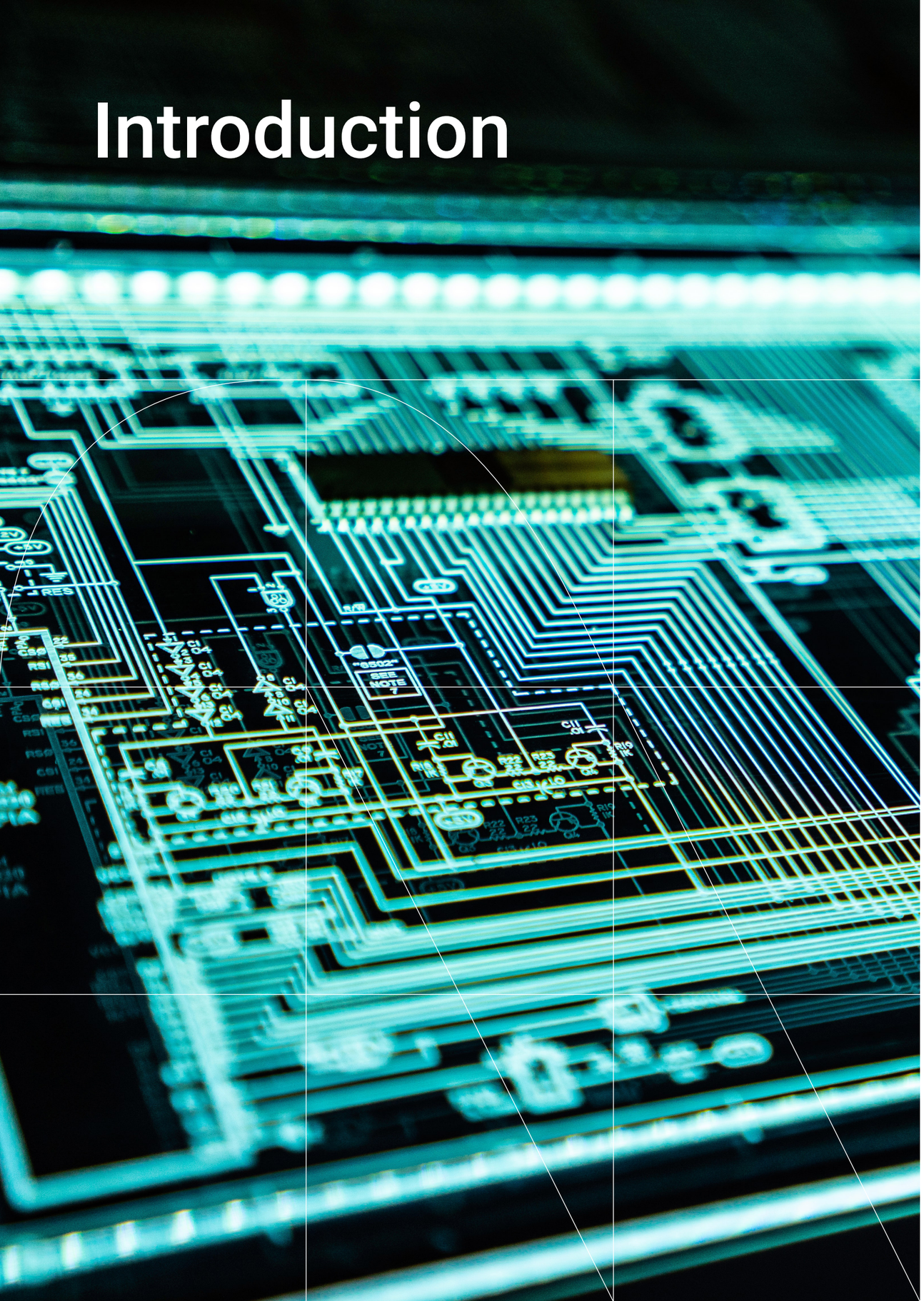
1. Insurers are one of the main targets for cybersecurity attacks. Companies in the industry are therefore expected to secure insurance products and services as well as im prove data privacy of the Personal Identifiable Information they store.

2. The Insurance industry faces four major cybersecurity challenges: cloud security, data-driven business, smarter and more automated and digital workforce. These are to be the top-of-mind priorities of insurers in their security agendas.

3. When dealing with cyber threats, prevention and preparedness are critical. MAPFRE, CNA, SegurCaixa and Chubb as some great examples of cyber emergency response plans.

4. NTT DATA offers end-to-end cybersecurity consulting .and implementation services. Some of these include: strategy, security, governance and risk management, privacy and security by design, remote monitoring and rapid response, cyber solutions, and cybersecurity awareness and talent.

Introduction



As the insurance industry becomes a data-driven business and companies operating within it understand the need to base their strategies on actionable and real-time data, the target they represent to cybercriminals also grows.

Insurance organisations have in their hands enormous amounts of sensitive client information representing a clear interest for hackers and nation states. Cybersecurity, then, rises as one of the biggest insurance challenges with insurers' prioritizing it in their decision-making.

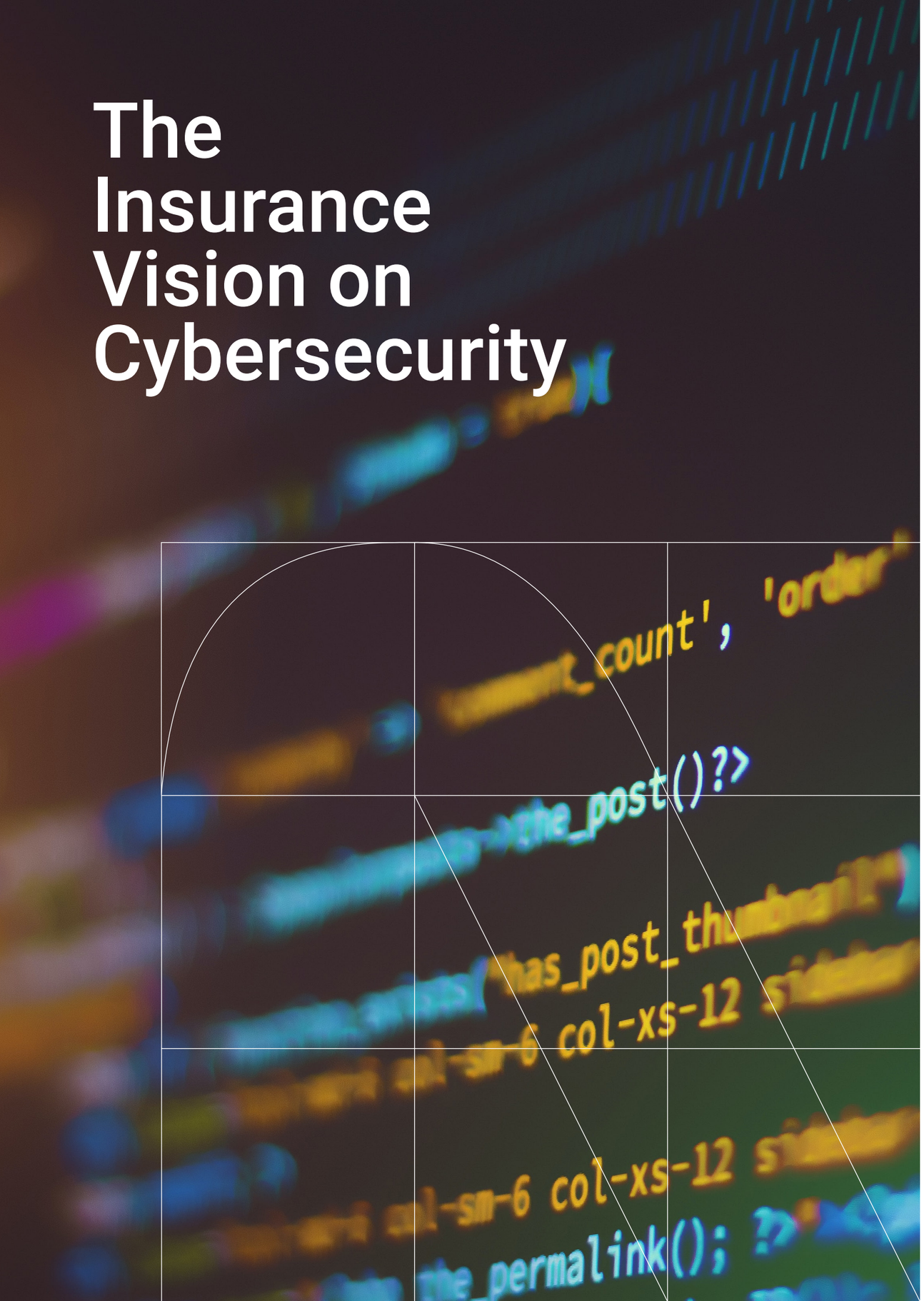
In parallel, the insurers' digital journey has increasingly accelerated their need for process automation to reduce work hours that do not add value to the company's overall performance. This is either by implementing intelligent tools or relying on human effort for risk detection and mitigation. For both options, security must be considered as an unavoidable and non-negotiable premise.

Furthermore, gaps between business and technology continue to close and insurance companies have realized that cybersecurity has become a business risk. This means, it can no longer be taken for granted nor relegated to level two concerns. CISO's (Chief Information Security Officer) are now responsible for top-tier decisions, and work hand-in-hand with CxOs to lead in the face of unexpected operational risks.

All the above along with ongoing changes and extremely demanding requests from policyholders, make the cyber scenario a room of full debate and continuous testing.

NTT DATA's insurance capabilities and holistic approach to security allow us to leverage our expertise and knowledge in the present white-paper and provide a series of trends, challenges and examples of best practices regarding this hot topic. This report highlights an overview of the insurance cybersecurity landscape across different regions and the areas of opportunity where insurance companies need to focus in order to be able to thrive in an era where technology and data privacy are necessary for survival.

The Insurance Vision on Cybersecurity



Cybersecurity is a big challenge for today's insurers as they undertake digital transformation. The more data they store, the higher the value they represent to nation states and attackers, especially when it comes to Personal Identifiable Information (PII).

In addition to the global challenge of integrating technology in the companies' service offering, operations, and management, enterprises ought to be aware of another cross-industry dilema: responding to unexpected events. These events include all unforeseeable situations that might deliver porential risks such as: a pandemic, natural disaster, climate change, third-party risks, ESG related risks, or our focus in this paper, cyber attacks. New operational risks arise from these unexpected situations and need to be considered in the industry's products and services, requiring these products to be updated by insurers, who are requested to be able to give quick responses on these matters.

Cybersecurity gives rise to four specific, non-exclusive challenges which insurance companies ought to pay attention to. These include:

Cloud security
As cloud migration has become a priority for insurers in the latest years, cloud security emerges as a new need to put at the top of enterprises' risk management agendas. Optimizing their operations by moving to cloud requires insurers to be able to balance productivity and security. These new technologies undoubtedly help organisations by providing new features and increasing scalability beyond their in-house infrastructure but have consequences if not approached with security standards on mind.

However, managing security in the hybrid and multi-cloud environments favoured by enterprises is complex and requires methods and tools that work seamlessly across public cloud providers, private cloud providers and on-premises deployments.

Data-driven business
Insurers are now required to worry and take care of their customers as they base their strategic plans and decisions on customer's data. Insurance companies need to be data intelligent to move faster and keep pace with the other acceleration forces that may provide a competitive advantage in this modern environment. Insurance companies need to be as agile as possible and quickly adapt to the opportunities, but also the risks, constantly appearing in this landscape.

Those that succeed in becoming completely data-driven companies enjoy increased revenues, greater efficiencies, and improved profitability. But as they become dependent on data, it is imperative that they have a holistic strategy covering areas such as data compliance, governance, data privacy, resilience, audits, etc.

Smarter and more automated
While several tools might be implemented to effectively safeguard technology as email, antivirus/anti-malware, application security, data encryption, network and firewall security, VPN, among others, human intervention in terms of security will still be needed when it comes to raised alerts and incidents.

Moreover, while tools can also be improved to eliminate false positives, challenges occur when too many false positives are detected, and much human effort

is then required. Automation of time-consuming and repetitive tasks using intelligent technologies allows cybersecurity teams to concentrate on more productive activities and helps identify deficiencies that can be corrected using formalized procedures. Likewise, it eases tool standardization, avoiding the use and implementation of a vast variety of security tools which lead to higher expenditure.

Security automation consists of identifying threats in different cyber-environments, triaging potential alerts by following decision-making methodologies previously established by expert analysts and determining which action to take in response to these threats. All these in a matter of seconds, without the need of human intervention. With this, repetitive, time-consuming actions become way less time consuming and, so, more optimized.

Digital Workplace

It is not news that remote working has become a constant for companies worldwide. As more employees work dislocated from their offices, traditional security methods that rely on perimeters, passwords and manual permission management have proved both old and insufficient. Teleworkers are an increasing target for phishing, malware and password attacks, among many other cyber-threats. Therefore, companies especially those in insurance working with strictly sensitive data, must carry out the corresponding security procedures to prevent future problems.

With this regard, insurance companies have already undertaken Role Based Access Control (RBAC) methodologies, and put Zero Trust approaches as a priority when securing their remote workplace. This assures all workers whether connected to the organisation's network or not, or connected to a local, cloud or hybrid network to be authenticated, authorised and validated when accessing applications, data, and documentation.

These are the 'Big Four' challenges when analyzing the top-of-mind priorities of insurers in their cybersecurity agendas. The above are the 'Big Four' challenges when analysing the key priorities of insurers' cybersecurity agendas. They also entail the crucial management and operational actions organisations need to focus on. But also, the central actions they need to focus on within their companies across their management and operations. Security is a double-edge sword: an offer and policy, something that companies must provide their customers with, and an internal focus they must guarantee taking care of.

.

Digital Maturity Spectrum: The Organisations' Journey Towards Complete Digitalisation

Insurance companies have been migrating toward digital technologies for some time now with the objective of maintaining long-term customer and supplier relationships, expanding in new products and markets with greater time-to-market, and providing higher shareholder value. In addition to pre-existing market trends of consumerisation, margin pressures, and ecosystem integration, the pandemic brought in remote work and online stakeholder engagement, which means insurers have now adopted communication technologies in addition to digital channels and value chain automation.

This impromptu maturation of digital technologies has certainly brought up several opportunities for the insurance business, such as personalisation of products and services, real-time attention and monitoring, virtual team management and smart working. However, this rapid move towards digitisation has also led to a dramatic increase in the number of successful cyberattacks experienced by the insurance industry.

Insurers are now responsible not only for securing their digital channels and safeguarding data, but also securing their legacy technologies. Many insurance companies still have a mix of digital and legacy technology in their business processes. Despite this, fewer than 25% of companies have truly digitised value chains based on a [1]recent survey of 200 largest worldwide insurers conducted by ACORD, fewer than 25% have truly digitised value chains.

The Role of Security in This Digitisation Landscape

A successful, growth-oriented company must adopt digitisation strategies and promote connectivity between devices and people. However, it must simultaneously take action by vigilantly observing the safety of its information systems.

Insurance companies need to collect In-depth information about policyholders including historical information, Professional Indemnity Insurance (PII), financial and health information which makes them an undoubted target for cyber criminals.
The main cyber crimes in insurance include: ransomware, social engineering e.g. phishing attacks, Denial of Services (DoS), complete service interruption, data leaks and breaches.

With this in mind, cybersecurity has become a business imperative for the insurance industry as cyber risk is a top operational risk faced by the sector. Traditionally, cybersecurity was deemed as an IT risk with the security organisation embedded within the CIO's organisation which resulted in limited budgets and resources for cybersecurity and at times even conflicting priorities.

Nevertheless, based on emerging cyber threats and risk to the sector, many insurance companies now realize that cybersecurity is a business risk. In the revised organisational structure, CISO now reports into the CEO. There is often board level support with budget and resources for managing cybersecurity risk and insurers are taking a strategic approach to address cybersecurity. There is a shift from the traditional compliance and 'checklist' mindset to proactively managing cyber risks early on in the software life cycle.

As a top-tier decision-maker, the CISO, along with other CxO's must first carry out a cyber risk assessment and map the vulnerabilities that might be implicated in the different insurance businesses and evaluate the potential damage. Afterwards, reactive strategies must take place in form of a Cyber Emergency Response Plan, to guide the specific actions to be taken in the event of a cyberattack.

Successful, growth-oriented companies must adopt digitisation strategies and promote connectivity between devices and people. And simultaneously taking action by observing the safety of its information systems.

Cybersecurity has become a business imperative for the insurance industry as cyber risk is a top operational risk faced by the sector.

DevOps and Security: Integrating Security Early On in Development and Delivery Cycles

As each insurance company is free enough to implement DevOps processes differently, they are also responsible for establishing a RACI matrix with identified roles, associated responsibilities, and ownership. Some companies have evolved to the extent of introducing DevSecOps, embedding security earlier in the development lifecycle. Additionally, application launch is accelerated in each phase of the process while carrying out some security functions such as identity management, firewalling or vulnerability scanning.

Besides checking security vulnerabilities throughout every stage of the process, DevSecOps leverage other great benefits to the insurance industry. They enable competitive advantage by quickly processing insurance claims and offering accurate quotes, automating inefficient processes to eliminate wasted labor hours and rapidly produce quality products or ensuring regulatory compliance. DevSecOps processes also help turning data into workable sets and therefore, reduce errors while generating useful analytics and actionable feedback as well as guaranteeing well-structured code, yielding to successful deployments.

On the other side, however, DevSecOps may DevSecOps may face some challenges, especially when taking into consideration the workforce implicated in the security processes. According to [2]Gartner, there is a clear need for retraining developers, but insurance companies need to keep in mind that they cannot "force information security's old, heavyweight, checkpoint-focused processes on DevOps developers", but rather "integrate continuous security assurance seamlessly throughout the CI/CD toolchain and processes".

Likewise, says the analyst, DevSecOps imply a change of mindset and development culture process, going from one-time gating using security scans to a continuous security assurance process". Nonetheless, the idea of creating zero-vulnerability applications slows developers and takes time to fix low-risk vulnerabilities, so Gartner encourages developers to focus on the most important security issues identified through threat modeling.

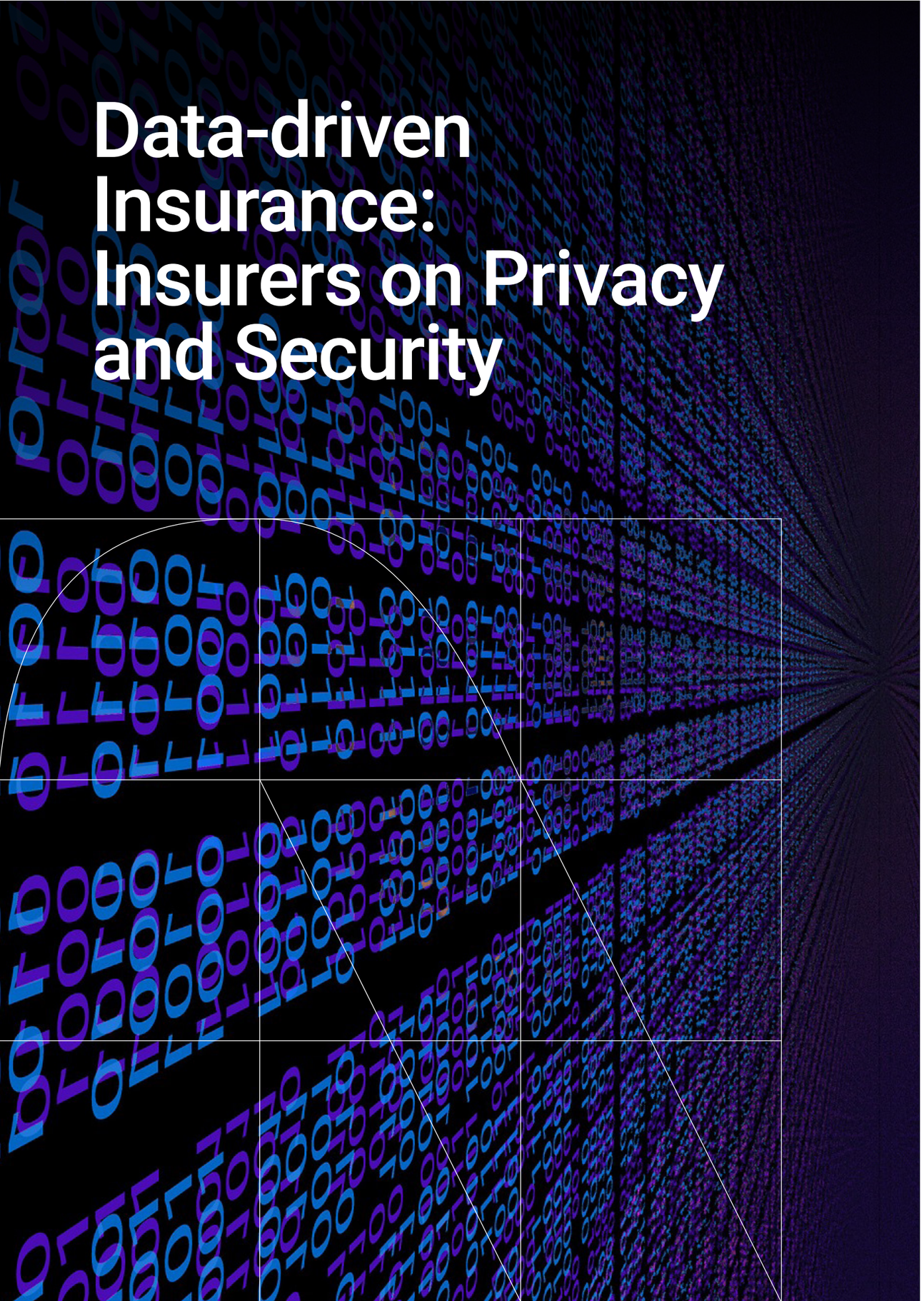
Moreover, our approach to security in the software lifecycle is based on the implementation of a secure development model (based on OWASP SAMM), which establishes all the security requirements and controls that must be carried out in each phase of the SDLC. From this model, the security organisational structure is created, based on a security office for project security supervision, and the generation of Security Champion profiles (security coordinators within their team).

This security office is in charge of integrating security controls within the project or company's CI/CD to establish the security controls to be carried out by the projects in each phase. It is the responsibility of the office to execute and supervise the results of these tests and, together with the Security Champion, manage the resolution of the action plan on the detected risk.

This whole process must be monitored through a dashboard that allows to analyze the level of compliance of each project and/or Security Champion with respect to the secure development model generated for that context. In this way, it is possible to detect areas of non-compliance and direct efforts in an appropriate manner.

Automation is a tool that allows to scale the number of controls carried out, but from our point of view, management is key to achieve an improvement in the level of risk.

.



Data-driven Insurance: Insurers on Privacy and Security

Insurers as Targets for Cyberattacks

As already seen, digital transformation has much to offer the insurance industry. A data-led approach enables the creation of new revenue streams, accurate underwriting, decreased risk, optimised and personalised customer and partner relationships. The drive towards improved customer experience and speed to transaction has resulted in the insurance industry focusing on application development and automation with data being at the very heart of the industry. Data and automation are making insurance "smarter", thereby allowing it to quickly adjust its rates to reflect the results of data analytics and identification of exposure trends. Smart sensors in cars or personal fitness devices providing additional lifestyle telemetry that might impact health insurance or auto insurance. Consumers major concern around privacy may be counterbalanced by a desire for lower premiums. The increased reliance on digital enables insurance to be more successful but it also exposes increased cyber risk, therefore the insurance industry is stepping up to the challenge. Consumers need increased assurance that insurers are handling their data securely, appropriately and in line with privacy requirements.

However, the digital transformation of the insurance industry has been hampered by legacy systems and highly manual processes. The pandemic has highlighted this and there has been a growing focus on digitising processes and systems within insurance. According to [3]Gartner's article How Leading Insurance Companies Manage Legacy Modernization, insurance companies with high digital maturity were twice as likely to perform better than planned against their core system modernisation goals than companies with low digital maturity. However, around 50% of insurers have 50% or more of their core insurance systems utilizing legacy systems. Gartner has also found that 65% of IT budgets are allocated to "run" the business. The most successful insurance companies will be those that automate and that are able to provide an efficient and personalized service.

Various challenges are faced when considering security as a top-of-mind priority in insurance:

Increased Regulatory Pressure

Technological advances are introduced at a very fast pace, especially as we move towards an Open Insurance scenario Additionally, there are insurance indusrty regulations which have also emerged with the same speed and strength. As we presented in our [4]Regulations paper within the Insurtech Global Outlook 2022 Report, there are many regulations that affect the insurance industry both directly and indirectly. Some of them, although with local applications, are global, such as Solvency or IFRS 17, and many others have a national or state component. Despite this, insurers worldwide are being affected not only by the attacks previously remarked, but also by the need to comply with all the regulations that have been born since.

Many state and federal governments globally have enacted data privacy laws not only to safeguard consumer data from malicious actors but also to prevent misuse of consumer data in the business operations of insurance companies. Non-compliance with these privacy regulations may subject insurers to civil liability, financial penalty and also damage their reputation, making it difficult to retain and attract new customers. Therefore, staying in com-

pliance with these laws and safeguarding consumer data is the top priority for insurers. Some things that insurance companies can do to make sure that they are safeguarding consumer data is make sure that they are aware of the privacy regulation in effect for their geography, educate their internal stakeholders on the use of data in alignment with [5]FIPS principles, improve their security posture, and beware of and address consumer concerns of data privacy.

1.DATA PRIVACY & PROTECTION REGULATIONS

In recent years, different laws have come into force regarding the protection of access and processing of people's data. Undoubtedly, all of them have different scopes due to each country's situation. In some cases, they are more restrictive rules and in other cases they are less demanding when it comes to requiring obligations from companies when handling personal data.

The most important privacy law created so far is the European **General Data Protection Regulation (GDPR),** which came into force in 2016 but was not applied until May 25, 2018. This has led to the development of many other laws around the world based on its standards, that demand all companies that operate with personal data of European Union citizens to apply strict protocols to ensure the proper use of the data.

Despite its relevance globally, GDPR is not the only regulation surrounding data privacy. In North America, for instance, the **Gramm-Leach-Bliley Act (GLBA) or Financial Modernisation Act of 1999** controls how financial institutions in the United States (commercial banks, investment banks, securities firms, and insurance companies) treat the private information of customers. Meanwhile, in Canada, they have the **Personal Information Protection and Electronic Documents Act (PIPEDA)**, a federal privacy law aimed at private sector organisations.

In Latin America, the **General Law on Protection of Personal Data of Brazil** stands out, and in the Asian continent many are their specific legislations: **South Korea's Personal Information Protection Act,** China's **Personal Data Protection Law**, or Thailand's **Personal Data Protection Act**. In the case of Japan, the **Japan's Act on Protection of Personal Information** is scheduled to come into force in 2022.

In terms of data privacy, therefore, there are great data privacy differences when it comes to regulation. Depending on the country or region, standards are required with different magnitude and strictness. But what is certain is that all these laws seek greater protection of people's rights against the use of data by companies as companies are being increasingly aggressive due to the use of digital platforms to market their products or services.

In the case of insurers, the situation is not very different from that of other sectors, since they have to guarantee that they comply with the aforementioned laws or regulations. To achieve this, they can develop their own solutions or leverage partnerships with third parties. These are usually third parties who expertly know how to apply technology to meet regulatory, security and compliance requirements or needs. Although they must also have other large partners, such as cloud service providers, who are responsible for processing and managing huge amounts of data from insurers.

2. RISK MANAGEMENT REGULATIONS

The European Parliament and European Commission presented in September 2020 a legislative proposal for a regulation on digital operational resilience in the EU financial services sector. The future law **Digital Operational Resilience Act (DORA**) seeks to strengthen and update the risk requirements posed by Information and Communication Technologies (ICT) in the financial sector, including insurance and reinsurance companies, to ensure that all stakeholders in these industries operate under a common system to avoid the risks derived from the use of certain technologies.

DORA aims to ensure that all participants in the financial system have the necessary safeguards to mitigate cyberattacks and other risks. The proposed legislation will require companies to ensure they can withstand all kinds of ICT-related threats and disruptions. The proposal also introduces a monitoring framework for critical third-party providers, such as cloud service providers.

The objective is that all members of this industry, including ICT service providers considered potentially critical, have the necessary procedures to be able to combat cyberattacks and other types of risks. Thus, companies must demonstrate that they can deal with digital threats and their effects, such as the interruption of their services. The new law will not only be directed at companies (banks and insurers), but it aims to extend its effects to companies that provide services to the former, so critical providers such as cloud service providers will also be subject to this rule.

One of the novelties of this law is that it will serve to harmonize the current laws on this matter, which are currently disseminated in different provisions. On the other hand, the presentation of this proposal also shows an objective of convergence between institutions, since the European Insurance and Occupational Authority (EIOPA), European Banking Authority and European Securities and Markets Authority (ESMA) have actively participated in its preparation.

The Need to Detect Threads and Quantify Risks Faster

More and more unexpected events must be considered to foresee their impact and act accordingly, prior to the damage. However, these unpredictable situations occur more frequently, driving the need for faster risk and vulnerability detection The same goes for scenarios that aren't necessarily uncertain but demand more attention to make faster actions. Such is the case of climate change.

As the uncertainty landscape is fast evolving, the need to detect risk increases. Insurance organisations need mechanisms for faster detection, quantification and mitigation of risks Companies must therefore make sure all stakeholders are involved within the risk management culture to mitigate communication risks as they arise and continuously monitor possible risks. Finally, if a risk ends up being materialized, then insurers need effective response and recovery.

Some typically used risk mitigation tools include Risk Assessment Frameworks (RAF), which facilitates an outline of systems that could be at low and high risk, and others as probability matrices, SWOT or root cause analyses.

The likelihood of unfavorable events occurring can be reduced, and quicker returns to normal operations can be achieved by managing business continuity plans

on a Governance, Risk and Compliance (GRC) platform —aligning its IT and business objectives, while managing risk and meeting regulatory compliance requirements. Business interruptions can therefore be planned for, therby reducing their frequency and impact.

Business continuity can be assessed with the same simplicity as third parties. To determine the availability and criticality of an asset, you can conduct risk assessments. The next step is to examine and identify resource dependencies by connecting assets, controls, and policies. Conduct business impact evaluations as well to determine the financial effects of disruptions. The GRC platform will highlight impacted areas that need to be addressed if a member of the recovery team departs from the company.

Fraud and Money Laundering

As the need for customized CX and competition in the insurance market increases, malicious purposes such as fraud and money laundering also increase. As established in our [6]2022 Insurance Vision, the global battle against fraud is one of the top three major challenges in the insurance industry.

Please change to: For the insurance industry, fraud is still latent and has only gained more relevance and attention because of the COVID-19 crisis. The [7]Coalition Against Insurance Fraud estimates that fraud costs the U.S. industry $80 billion in losses across all lines of business annually.

There is an increased industry-wide focus on value chain automation and straight through processing, which means fraud detection must happen in real time with the assistance of data and ML/AI technologies. There was an uptick in fraud during the pandemic despite reduced use of vehicles and commercial property as well as temporary shut-down of non-critical services industry. Increase in fraud means direct impact to profitability and increased premiums for policy holders. Insurers are shifting toward the use of ML/AI technology in early fraud detection.

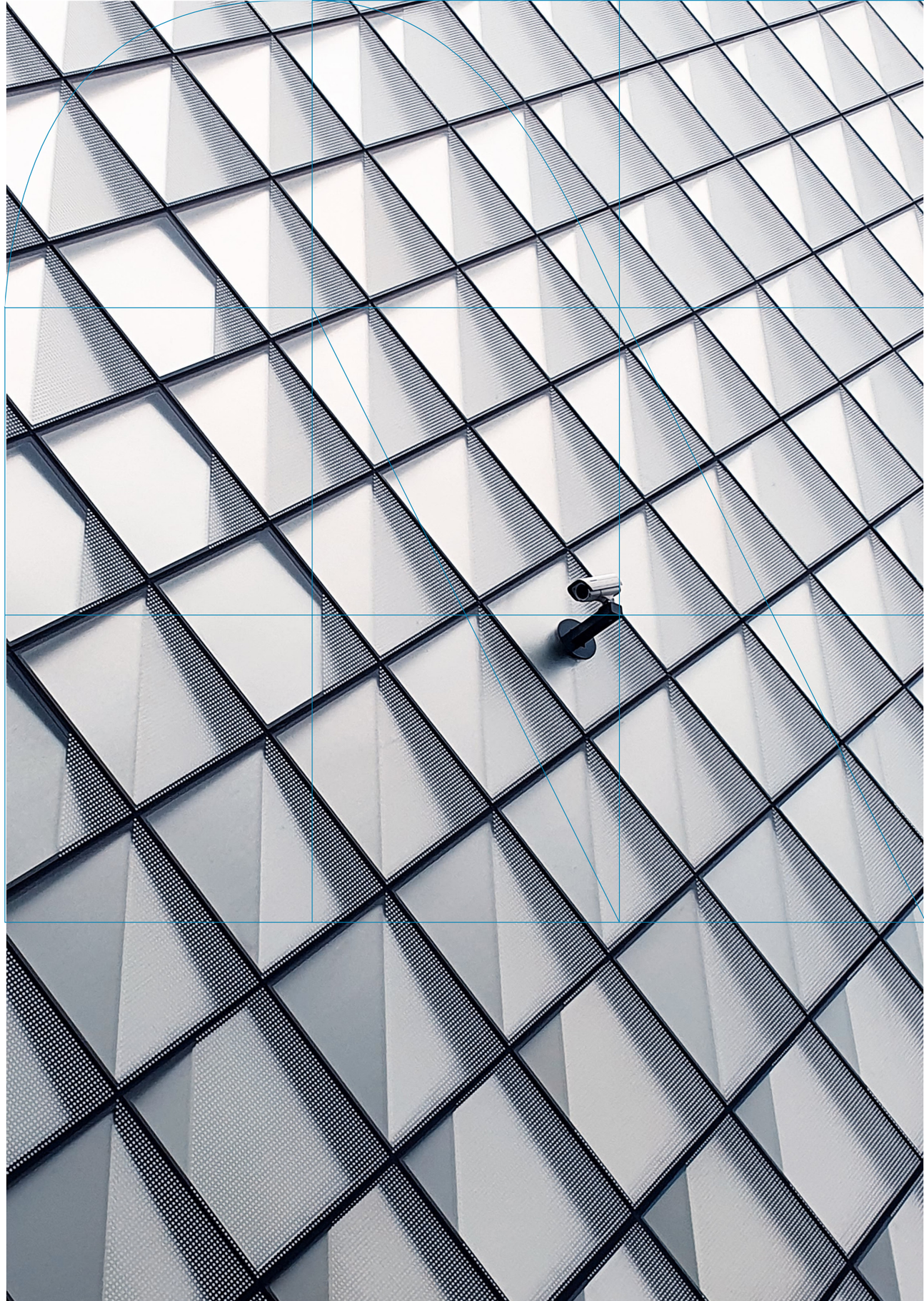
Cyberattacks

The main areas that represent a potential cyber threat are customer portals, credit card transactions, cloud data storage, B2B and B2C portals, data lakes, regulatory risks, application specific attacks, client information including security controls and insurance details, among others.

Hacktivists have been known to target insurance companies for ideological reasons and the PII of B2C policyholders is also useful to state sponsored threat actors because of the amount of detail that it contains. Insurance company breaches result in cybercriminals being able to find the policy details and security standards of their cyber insurance customers and use stolen information for fraud or cyber-attacks later down the line. State-sponsored threat actors can also use stolen information in intelligence and investigative operations.

State-sponsored intelligence services collect PII and ingest it into searchable databases against which they conduct targeted queries which allows for additional attack vectors.

Application specific attacks are also a key threat. It is human to make errors but errors in application coding can result in vulnerabilities that open the organisation up to attack. The organisation needs to build full cycle security controls starting with threat modeling and including penetrations testing and web application firewalls.



Securing Insurance

With all these challenges and demands, security is critical in the insurance industry and a must-do for organisations. However, security comes in different shapes and sizes with the 'one-size-fits-all' narrative reducing in organisations.

Therefore, insurance can be secure in the following ways:

Security By Design
The insurance sector must take action and begin to include cybersecurity concerns into all stages of the product or service development life cycle. Designing for customer experience, availability, security or privacy need to be highly considered. The foundation of the IT architecture powering the business must be a Zero Trust framework, already introduced in the beginning.

Data Security
It is impossible to create an entirely risk-free workplace. Encrypting data is a crucial security need in a Zero Trust environment for use, transmission, and at rest. In a sector that holds and processes crucial PII, solutions like Microsoft Information Protection that enable the deployment of policy-based encryption are essential.

Identity
The foundation of all security is identity. If you haven't verified the person accessing your system is indeed who they claim to be with an appropriate level of assurance, you can't build trust. All insurance companies should follow the strategy of attempting to establish an identity source of truth and identity and making sure that provisioning and deprovisioning, especially for privileged accounts, is subject to safe processes.

Passwordless Authentication
Cyber underwriters are becoming more and more concerned with proper security standards, and many of them now require multi-factor authentication. It is understandable that the insurance sector is pushing for strong, preferably password-less, authentication for both internal use and B2C and B2B engagements.

Risk Management and Strong Governance
Risk management is at the core of insurance, thus managing cyber risk should be a part of the organisation's enterprise risk strategy. A shared responsibility paradigm emerges from increased use of third parties like cloud service providers and software such as a service providers. A solid governance layer is necessary for all outsourcing methods in order to help the organisation get the greatest results and match the risk it is willing to take.

Business Email Compromise and Phishing Attacks
Email remains a popular attack vector. We can help users make better decisions by using technology that provides security controls to filter or highlight emails that are potentially risky. To achieve highly secure business emails, you should use DMARC, SPF and DKIM in combination. Marking external emails as [External] can be helpful as well as encouraging internal communication on IM like Microsoft Teams or Google Chat so that email is used only for external emails. In addition, run regular phishing tests and create a security culture that encourages good risk decision-making.

Network security is reliant on the remote and highly distributed nature of insurance sales. Secure Services Edge technology can help reduce the costs and security risks associated with vendor management while maintaining strong security measures. A Zero Trust networking approach can help keep sensitive data secure by encrypting and monitoring all network traffic.

Insurance companies use risk assessments to understand potential problems and provide the best possible protection for their customers. As a result, cyber insurance is becoming more common among insurance companies. This insurance is the coverage that a company can obtain to protect against losses caused by cybersecurity incidents. As cyber insurance an offering provided by more insurers, the client security requirements are becoming more stringent. An insurgence in successful attacks and state-sponsored cyber attacks increase risk and affect requirements that insurers must implement before insuring their organisations.

The insurance industry needs to reduce payouts and by its very nature, underwriting identifies areas of risk and excludes coverage for clients who have large exposure to potential vulnerabilities. Insurers are excluding coverage for losses if clients don't have multi-factor authentication. This is driving the cybersecurity controls that companies have to implement to remain insurable.

Due to the current challenges and demands the insurance industry has to overcome, security is critical and a must-do for organisations.

Cyber insurance is becoming more common among insurance companies to provide the best possible protection for their customers.

Building Trust and Reputation in Insurance: The Importance of Transparency for Clients

Building trust among potential and existing customers has always been a top-notch concern for the insurance industry. This may be a result of the insurance's nature, complex offering, and associated pricing models that has fueled a sense of mistrust among clients.

Additionally, there's increasing concern that user may share their personal data to companies of various types, markets, and industries. While data-driven insurance brings enormous advantages advantages including: improved customer experience with tailored solutions, increased targeting of existing customers, precise risk identification and new coverage, it also comes with consumer skepticism.

More and more consumers expect insurance providers to be transparent and provide a clear and unmistakable overview of the insurance policy information. This enables them understand what it covers, the benefits over other products and heightens consumer engagement.

But how can insurers guarantee full transparency and gain the trust of their consumers. To attain this confidence among policyholders, consider the following:

Putting Privacy and Security as a Number One Priority in the Decision-Making Agenda
Technology and business go hand-in-hand, and so must security and business. Privacy must be attained at a directive level, with leaders understanding it and giving attention to it as they would any other headline initiative.

Updating Systems, Processes and Operations
Insurance companies must not only evolve their existing procedures but also create new ones to ensure they are correctly using the data retrieved from clients. This implies starting to think about building new infrastructure and capabilities (human, financial, and technical) to make data actionable while guaranteeing the utmost ethical behaviour.

Continuously Adapting to New Norms
The regulations pointed out before are just some of the ones currently marking the legislative panorama of cybersecurity. However, norms in legal bodies in various regions are evolving as you read this paper. They are trying to actively adapt to the ever-growing technological, product, and service advances in the industry. Insurers must therefore take action on liabilities before they are required to, thereby leading the balance between data capitalisation and data ethics.

Overall, honesty truly is the best policy when building trust with exisiting and prospective customers. Granting users with a self-service UX and hassle-free information, as well as a complete understanding and visibility of when, where and how their data is being used, will aid insurers in generating trusting relationships with them.

Insurance Cybersecurity Best Practices

Human-centric Risk Management

Addressing the human side of risk is one of the most effective yet undervalued risk management strategies. Employees often click links in phishing emails, and are manipulated to provide access and information during social engineering attacks. They may also use weak passwords, accidentally download malicious hardware, or engage in frequent errors that cause security incidents. It comes down to generating the workforce's proper awareness, knowledge, and behavior to mitigate these risks.

As cybercriminals exploit these weaknesses to hack into sensitive information, incredibly 88% of security breaches result from human error, and 37% of attacks involve emails and letters as the root cause of breaches, according to [8]Stanford University's research Psychology of Human Error. To strengthen information security protection, companies must focus on better preparing their people. While investment and focus should continue, specifically on IT infrastructure, controls, and CISO-driven programs, the human factor remains a considerable risk. We see three areas of focus that organisations can immediately prioritize to start making an impact.

Align Leaders and Create Visibility from the Top

Overall, the direction needs to be aligned with the strategy and business goals of Chief People Officers and Chief Learning Officers. Forming a tighter and more formal link with Chief Risk Officers creates alignment for human-centric strategies focused on culture, awareness, and training specific to their company's enterprise risk profile.

Embedding a risk-based culture starts at the top. Leaders educated on specific risks can act as an accountable voice, promoting and communicating the importance of security. Companies must ensure that leadership is the face and voice of security as they lead by example in meetings and everyday behaviors.
Especially during challenging and uncertain times, Risk Managers have an opportunity to act as champions for an efficient risk management program. For example, during the beginning of the COVID-19 pandemic, teams turned to leadership for direction, transparency, and, most importantly — a plan. Strong leaders took this opportunity to evaluate risk and develop a strategy to protect customers, organisational assets, stakeholders, and employees.

Build a Security Culture across the Organisation

Most leaders understand that employee change and compliance doesn't happen in one day or with one training program. Instead, the best companies embed information awareness and risk-driven security into their culture. Culture drives beliefs and actions beyond what the best design controls can accomplish. Culture, as it relates to driving behavior, can be a "fourth line of defense" in managing overall risk. Therefore, leaders who wish to foster long-term behaviors must put risk as a focal attribute.

The first step to enacting sustainable cultural transformation is through awareness and education. Organisational risk awareness campaigns bring increased visibility to security threats and the associated risks through videos, newsletters, articles, and other mediums. Next, leaders must identify policies and procedures to enforce data privacy and security and ensure there are consequences to reinforce the behavior. Finally, organisations can align performance management processes tailored to leaders' roles, including data protection and prevention.

Deploy Formalized, Immersive Training to Master Security Threats

Employee awareness and behavior rely on the quality and relevance of organisational communication and training programs. Organisations must revamp annual slide deck presentations to deliver engaging and realistic trainings that prepare teams for the modern risk landscape.

However, deploying mandatory risk and compliance training is not enough. If leaders want their teams to retain information, they can scale gamification techniques, such as leaderboards, to reinforce desired behaviors and increase participation. Training programs should be more engaging and relevant, moving away from dated e-learning courses. For example, scenario-based simulations bring awareness to different security threats and how to best respond in unique situations. Additionally, not all employees have the same risk profile, and as a result, training should be tailored across different roles and teams.

Lastly, make it personal. Personalised risk training deepens lessons and resources in protecting data. In these training sessions, employees may realize the importance of security protection in their lives outside of work to bring this mindset as they enter the workplace. This relatable content can drive engagement as employees learn to make their personal data more secure.

Some Examples of Insurers' Response to Cyberattacks

Cybersecurity is a matter of the public eye not just because the consumers' concern for their privacy is latent, but because it has already drawn some companies to the dark hole. Examples of cyberattacks on insurance companies are many, in both giant groups and corporations as well as local carriers

For instance, in the [9]United Stated, Chubb suffered a cyberattack back in 2020 personal data of their policyholders was stolen due to an unauthorized access to information by a third-party service provider. A similar scenario due to ransomware happened to American insurer, [10]CNA in 2021. In Spain, similarly, cyberthreat cases were reported by [11]MAPFRE and [12]SegurCaixa, who both suffered who both suffered ransomware attacks in 2020. Other companies as Pacific Specialty Insurance Company or AXA are also victims of historical cyberattacks.

However, the importance of highlighting these examples is to show how these companies reacted to the threats rather than shed more light on the drawbacks of cyberattacks and the challenges they produce.

The case of MAPFRE stands out significantly, due to different reasons. First and foremost, the company itself informed clients and the general public about the breach , thereby enhancing the company's transparency and client trust.

Secondly, since the company was quick enough to communicate the attack to the relevant body, in this case, the Spain Data Protection Agency, the entity carried out an in-depth investigation of the case, and concluded that it was possibly a phishing campaign.

And lastly, the Spanish insurer is commended for their quick response to the attack. Within 7 minutes of detecting system failures, MAPFRE activated a high impact protocal, initiated an incident Management procedure, and turned to the crisis committee. Less than half an hour since the executed attack, the company had already massively shut down its devices, non-essential servers and isolated some network segments.

Workers from the security team of the company worked all night long to identify the ransomware and disinfect the affected devices. In a matter of less than 7 hours, the attack had been controlled and solved. What is the conclusion of this? That MAPFRE was prepared for an attack like this (or any other attack highlighted above). Having a protocol and specific guidance of what to do in the case of a cyberattack may, certainly, reduce its effects drastically.

NTT DATA's Capabilities & Use Cases

The Security Offering and Management Insurance Companies Need

NTT DATA has identified several critical elements that risk leaders should consider as they get ready to support insurance organisations of the future. These are:

1. Include risk leadership to participate in the organisational and business strategic planning process. This activity allows leaders to discuss business priorities within the company's risk management objectives. Risk leaders can also offer their perspectives regarding emerging trends that will enable them to see risks or opportunities that others might ignore.

2. Re-organize the risk function to align with business units rather than organisational divisions or functions. Traditional risk functions were aligned to finance or operations, but aligning them to the lines of business, such as personal lines within P&C or Life within L&A, gives business and risk the opportunity to bring risk perspective early on in business decisions. It also allows the risk function to get educated on business aspirations and their challenges in conducting the first line of defense responsibility. Future risk functions should be more business-focused, adding value as part of the profit center.

3. Define clear roles and responsibilities within the first and second lines of defense. Despite the prevalence of the Three Lines of Defense model, there have been ongoing challenges with its implementation. Often there are challenges in establishing clearly defined roles and responsibilities within the three lines of defense. Second Line of Defense or Enterprise Risk Management (SLOD) should aim to complement the First Line of Defense (FLOD), typically business units instead of duplicating them.

4. Invest in advanced technology and the right talent. Most risk functions still use manual processes and/or legacy systems that inhibit faster data processing which is the key to effective risk management. Upgrading to new technologies allows insurers to automate manual tasks, process data faster, and generate key insights for evaluating exposures, responding to risks, and measuring the control performance. Organisations should shift the risk culture from just a reactive compliance checklist mindset to a more agile, proactive, and cross-functional setup leveraging the latest technologies for efficiency and effectiveness. If risk leaders are thinking of augmenting their teams, seek out talent with an understanding and expertise in business, analytics, and nonfunctional risks such as ESG, climate, and cyber threats.

NTT DATA's Capabilities

At NTT DATA, we believe that the best way to minimize and neutralize the risks of cyberattacks and other threats is to adopt a holistic approach based on specialized solutions and services designed to protect your equipment, networks and resources both on-premises and in the cloud.

We offer you a wide range of end-to-end services ranging from strategic consulting, security measure implementation, remote monitoring, and technical consulting, all backed by the best cybersecurity solutions from our partners.

Thanks to our accumulated experience in projects for clients across all industries, our network of Security Operations Centers (SOCs) and R&D resources, we have industry-specific knowledge and technical expertise to help you protect your business against cybersecurity risks.

Our roadmap to Cybersecurity services is based on five main lines of action:

Strategy, Security, Governance and Risk Management
We identify and manage your business risks and ensure compliance with data security and governance regulations specific to your country and industry. Count on us to reduce uncertainty and make better long-term decisions.

Privacy and Security by Design
With our automated security testing, security by design DevSecOps and Red Teams services you can improve the security of your software architecture and products.

Remote Monitoring and Rapid Response
Our Security Operations Centers (SOC) offer you monitoring and identity management services, network access control, incident detection and response automation in the Cloud.

Cyber Solutions
The main areas of our solutions implementation are identity management, access control in cloud environments, industrial cybersecurity and digital fraud.

Cybersecurity Awareness and Talent
We offer you continuous learning methodologies and awareness courses on cybersecurity related topics, all of them adapted to the specific maturity level of your organisation.

Use Case (Anonymous)

Client Need
For this Rule Reengineering Project, the client required the improvement of security ratings on firewalls in 22 countries in South and North America.

NTT DATA's Help
Thanks to NTT DATA's capabilities, the client outsourced the project end-to-end from the definition, planning, and operation of the new policies in the firewalls of the different countries, organizing the different areas involved and coordinating them to minimize the impact on the business.

Results and Benefits
As the project is still ongoing, we can not quantify the benefits. However, this security service focuses on improving and increasing the level of IT security in the following management groups, which are, then, the areas where we expect on having highlighting results:

- Operational security management.
- Infrastructure shielding management.
- Identity and authorization management.
- Incident management.
- Vulnerability and update management.

Similarly, the IT security service focuses on defining, planning, elaborating, deploying and verifying those system health projects identified as key to improve the company's maturity level on the group's security infrastructure. This is all through a risk management approach.

Conclusion

It's clear that insurance is growing quickly and changing constantly - it's an ever-evolving sector that's persistently being tested. As uncertainty continues to be an uncontrollable but omnipresent element of insurance, security will keep highlighting as a priority to focus on.

Companies in the industry must adapt to changing global conditions in order to stay competitive. Steps that must be taken to do this include thinking about how to best survive in these challenging times, while considering global and market related trends.

There are several things that security leaders need to be aware of and act on. These can vary from tools and methodologies use, team engagement, information utilisation, and technology and business need adaptation. However, if insurance leaders are to keep in mind four highlights of this paper for their agendas, they would be the following:

1. Security is a business challenge beyond technology. It has to be introduced in the decision-making of insurance organisations from the top, ideally from the Board of Directors.

2. Data privacy will always be demanded, both from the regulators and customers. Transparency and ethical management of personal information must be guaranteed end-to-end in the insurance contracting process.

3. Cybersecurity is not a final, gatekeeping stage. It should be integrated from the very beginning whileidentifying potential threats and vulnerabilities prior to their materialization.

4. Taking the above in account, prevision and response readiness are game-changer. Therefore, having a pre-established, clear and well-communicated protocol on what to do in face of cyberattacks is critical.

Our team of cross and insurance security experts, in addition to our executives' experience on market and industry worldwide trends, have helped in building this Thought Leadership on the matter. It includes areas where CISO's and CxO's should pay close attention to in the short term so as to respond to consumers' demands and thrive despite constantly emerging risks. These challenges, advantages, examples and advice will hopefully place insurance leaders as subject matter experts in the industry and guide them towards automated, data-driven, and secured insurance.

From NTT DATA, our global expertise in the insurance business allows us to build a founded strategic vision and to display specific advisory for insurers to be able to lead this digital journey. Our role as a multisectoral expert will provide companies within the industry with frameworks, tools and solutions to enhance their leadership in the market and, above all, go beyond the insurance scope.

References

1. ACORD Insurance Digital Maturity Study (2022 edition. https://www.acord.org/marketplace-pages/product-detail/acord-insurance-digital-maturity-study-(2022-edition)

2. 12 Things to Get Right for Successful DevSecOps. https://www.gartner.com/doc/3978490?ref=clientFriendlyURL

3. How Leading Insurance Companies Manage Legacy Modernization. https://www.gartner.com/doc/4014359?ref=solrAll&refval=334260698

4. Insurtech Global Outlook 2022. Regulations. https://insurtech-insurance.nttdata.com/four-forces/regulations/intro

5. Fair Information Practice Principles. https://iapp.org/resources/article/fair-information-practices/

6. The 2022 Insurance Vision. Going Beyond the Insurance scope. https://insurance.nttdata.com/thought-leadership/2022-vision/

7. Fraud Stats. https://insurancefraud.org/fraud-stats/

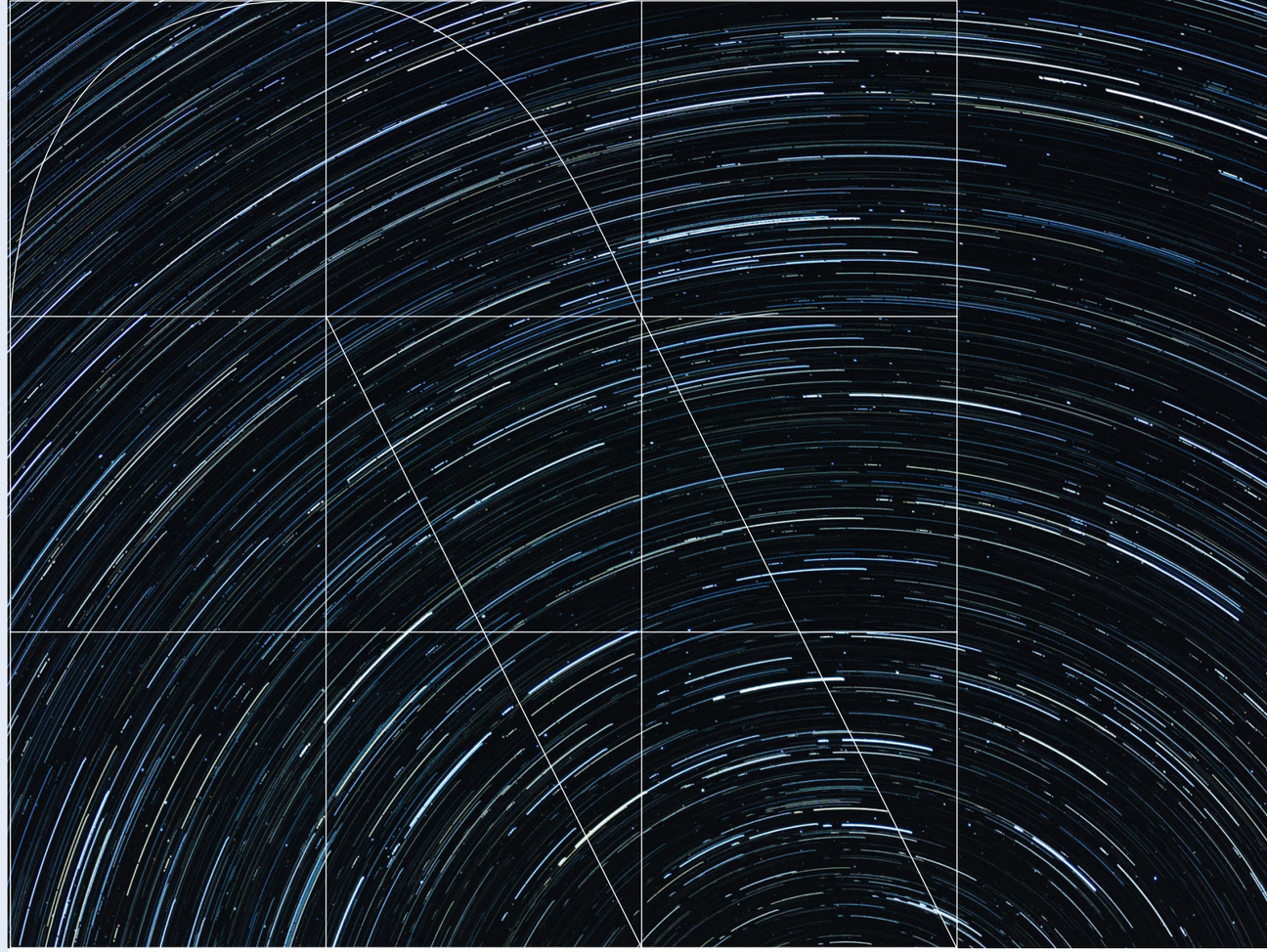
8. Understand the mistakes that compromise your company's security. https://www.tessian.com/research/the-psychology-of-human-error/

9. Cyber Attacks Against Insurance Companies: How to Avoid the Risks. https://votiro.com/blog/cyber-attacks-against-insurance-companies-how-to-avoid-the-risks/

10. CNA Paid $40 Million in Ransom After March Cyber Attack. https://www.insurancejournal.com/news/national/2021/05/21/615373.htm

11. Mapfre acknowledges being the victim of a ransomware cyber-attack: "We are doing everything humanly possible to continue providing the service". https://www.businessinsider.es/mapfre-reconoce-ser-victima-ciberataque-ransomware-698639

12. This is how a "ransomware" attack has affected one of Spain's largest insurance companies. https://elpais.com/tecnologia/2020-10-16/asi-ha-afectado-un-ataque-de-ransomware-a-una-de-las-mayores-aseguradoras-de-espana.html



NTT DATA

Natàlia Solé Riera
Head of Cloud + IM + Security at NTT DATA EMEAL

Enrique Bernao
Cybersecurity Manager at NTT DATA EMEAL

Sushila Nair
Vice President of Security Services at NTT DATA Services

Nutan Pandit
Practice Leader, Insurance Risk and Compliance at NTT DATA Services

---