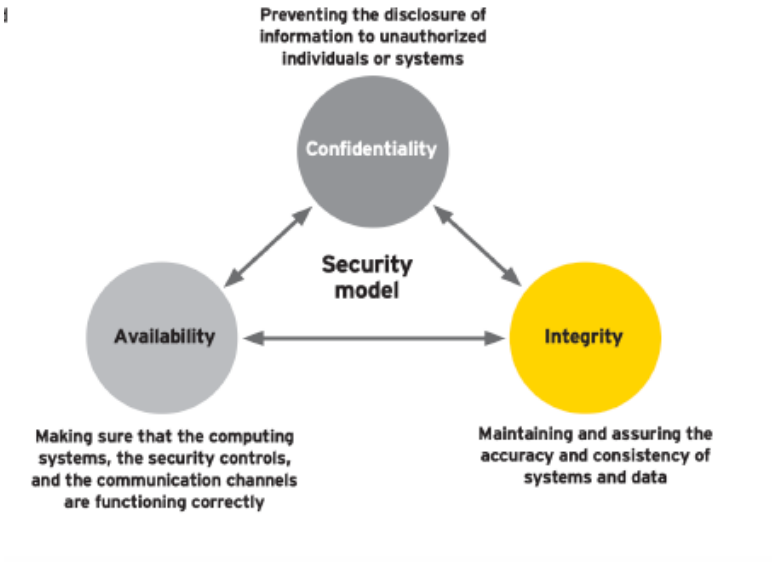
INTERNATIONAL INSURANCE SOCIETY

An affiliate of The Institutes | Risk and Insurance Knowledge Group

Where Cyber Insurance Meets Cyber Integrity

This paper focuses on cyber security and an industry perspective based on the importance and meaning of cyber integrity. Data integrity, storage repositories, device endpoints and the networks that serve them is the most important cornerstone of cyber security and will transform the market over the next decade as cloud computing, 5G networks and the quantum computing era evolve. These developments will shape understanding of cyber risk and improve cyber insurance by providing better cover by more accurately quantifying risk, mitigating claims, and evolving better risk management. The Ponemon Instituteii states that just 15% of digital assets are insured. The paper will not cover the whole cyberspace and cyber insurance overview as that has been done comprehensively by the OECD iii and SWISS RE SIGMA[iv] but to bring out the difference between data encryption or confidentiality with that of data integrity. This understanding is paramount for regulators, (re)insurance underwriters, and the c-suite of the customers they serve and is often a source of confusion. The diagram below shows the obligatory need to intertwine the cybersecurity triangle.



TENETS OF TRUST VERSUS TRUTH

To achieve the abstract, readers need to differentiate between definitions of trust versus truth. This is a litmus test as to whether or not data and networks have integrity and whether the

military mantra of “trust but verify” can be applied to these exponentially increasing intangible assets.

Trust is a strong belief in the reliability or ability of someone or something”. Trust in a network and the data stored in an enterprise or cloud service provider makes little sense unless there is basic instrumentation and metrics developing formal situational awareness into how reliable these assets are. This ecosystem needs snapshots over time into what they are doing with the data, services, and applications they are hosting. This is mutual auditability of liability. The INTERNET was not designed with privacy and security in mind, but communication between academia, so how can we trust in the status quo without verification.

Truth by distinction, is measurable with undeniable independent proof and is essential for any network, enterprise interacting with the data storage assets being hosted. There should be the ability to independently verify these assets with forensic proof that holds up in a court of law with attribution and non-repudiation. This cyber integrity instrumentation and the immutable evidence it affords should also be able to work at the storage scales required for all the data being generated on public, industrial and private networks estimated at a conservative 175 Zettabytes by 2025.)

REGULATION

Recent privacy law regulation such as GDPR[v] (General Data Protection Regulation in EU) and similar laws in Australia and USA bring out the need to look at mandatory data integrity, not just confidentiality, for first and third party data sources for organizations. They are accompanied by serious financial penalties for non-compliance. Countries not introducing this level of regulatory mitigation will have a serious weakness in addressing cyber risk and data breaches. It is not adequate to just encrypt data across an enterprise but to identify and tag key data pieces that could affect state sponsored attack, solvency of organizations and individuals should that data be breached. For companies this brings compliance of looking at data as an asset to the boardroom level. Regulators need to move to an priori approach of regulation from the current approach that depends only on experience and empirical evidence to provide a mathematical tautology to cyber risk independent of experience.

CYBER INSURANCE CLAIMS AND DATA INTEGRITY

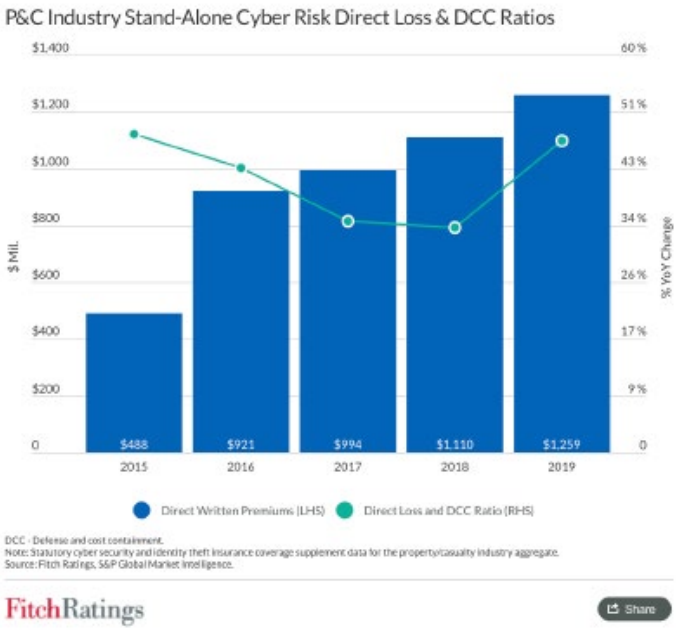
Cyber breach is an equal opportunity risk and individuals, governments or enterprises, face the negative effect of a massive outage in the cloud and the insurance industry accumulation risk across service providers who hold ambiguous liability in contracts. Substantial financial losses can occur as a result of multiple undetected events over multiple years and geographies so mitigation of accumulation risk is required.

Boardrooms, in general, lack a clear vision of the value of data assets at risk. For the insurance executive lack of supporting actuarial data complicates pricing and reserving with a constant need to accumulate sufficient claim event data. This affects earnings volatility and can create over reliance on assumptive models. However green shoots are emerging as traditional reinsurance is now being complemented by parametric structure innovation and capital market solutions. Such a shift requires granular data integrity to ensure contract certainty and avoid basis risk[vi].

Customers want immediate cash on a qualified breach event to recover quickly, moving away from cyber exclusions, which often prevent take up of adequate cover. Insurers want to reduce long running claims expenses and address aspects of the risk that may be deemed uninsurable. As the risk is digital in nature automation of first notice of loss (FNOL) using the alarm and detection, a real time property of data integrity, will enable early reserving of cyber claims from risk event signatures. Accuracy of the subrogation evidence generated reduces the estimations of incurred but not reported (IBNR) claims that can present a latent solvency event. Underwriters can pinpoint cyber risks such as active exploit, malware, ransomware , zero day trust and most importantly insider human error (accidental or deliberate) and develop automated claims processes around these from the data driven event signatures provided by their customers through the natural outcome of their operations.

When breaches happen, average cost to enterprises, has risen to $3.92M and cybercrime damages are expected to reach $6T by 2021 with cyber insurance premiums $20B by 2025. Claims cost of a cyber event averages about $4.88M (or more when you factor in pending claims and self-insured retentions) out of average economic loss of $8.64M per breach. Worldwide spending on cyber security will reach $133.7B in 2022 according to Gartner[vii] with less than 10% of that budget allocated to data integrity. Now we have to factor in any fallout from a pandemic in the hardening commercial market and correlate a potential massive cloud outage.

The recent graph from Fitch Ratings below shows an increase of cyber line loss ratio recently from 34% to 47% in 2019 close to 2015 levels. Without serious investment in integrity, cyber risk and loss ratios are likely to increase. Instead of increasing security perimeter complexity and trusting more secrets, this is a paradigm shift in security with instrumentation afforded from the inside out at the data-level, with real-time reporting for critical organizational applications and assets. This will allow the insurance industry and the organizations they back to better identify and visualize threats and changes to important intangible assets and data such as copy, transfer and deletion, as well as the manipulation of assets in real-time. *If we are investing more but performing worse, something is fundamentally wrong with the approach we are taking as a society to cyber security.*



QUANTIFYING CYBER RISK

Economies and businesses need a predictable, deterministic environment to grow, where risk can be quantified and managed alongside investment and return. The World Economic Forum[viii] and other sources believe the lack of functioning cyber security threatens as much as $9T of non-realized potential growth during this decade especially with the emergence of 5G networks in 2020 so robust cybersecurity must be addressed. Applications and software vulnerability risk is high especially when delivery of those assets has increased daily with velocity to provide new services.

Enterprises must assume compromise as even the most 'secure' infrastructures will be vulnerable to insider threat, insecure code and compromise by creative exploiters, attackers, and hackers. Governments, their defence establishments, or multinational corporations still require education for top management on how to bring transparency into how data is being stored, manipulated, and how it can be trusted given information rules outlined in outsourced service provider contracts.

PROVABLE SECURITY – an underwriting opportunity

The ideal for cyber security and cyber claims management is the undeniable truth (not trust) in the data, whose authenticity, identity and proof of creation time can be verified independent of the hosting or service provider. This is a dominant paradigm in cyber security research to reach a state known as "provable security". To satisfy this there has to be confidence in a security protocol backed by a mathematically rigorous theorem that establishes a conditional guarantee of security given certain assumptions. The challenge, and reason why provable security has remained in academia for so long is that it does not gather muster if the assumptions require the security of cryptographic keys or human trust as secrets in physical keys can be exposed and people compromised.

Provability doesn't matter much in practice if there are attacks that can defeat the security more effectively and these emerge all the time which has led insurance underwriting to chase trends rather than addressing the risk using data driven techniques. Integrity is where provability can be meaningfully applied. The public key cryptography (PKI) we use for confidentiality has integrity limitations and will be rendered ineffective as quantum computers emerge, to handle the burgeoning data. PKI invention[ix] did not have to think about integrity but key exchange for two parties to communicate securely across an insecure channel and is the foundation for the e-commerce and identity systems today.

Up to now PKI has been the only effective tool, and has served us well, but it requires secrets and trusted parties that can't be proven and remains the weakest link in security as intangible assets increase. Managing keys in a cloud environment is tricky and even the best security companies can't do it successfully which is the downside. The upside is that keys are not necessary for integrity and by eliminating their need and using widely witnessed consensus and evidence it is possible to have provable security which is a Eureka moment for security officers and insurance underwriters who want to secure their networks, data and provide/receive the proper insurance covers requested. They can now say "my network has integrity and I can mathematically prove it" rather than saying "my security is based on key management and trusting system administrators". Provable security will then become a standard in all insurance contracts and warranties. Cloud and decentralised local edge computing, offer a big dilemma in this regard and this is a risk mitigation priority for industry.

CLOUD COMPUTING DILEMMA

Cloud Computing is becoming mainstream, environmentally friendly, commercially important and efficient but high risk if we cannot manage physical keys in the cloud in a future proof manner. Large cloud operators such as Amazon, Microsoft and GOOGLE are well known but there are many outsource providers and emerging ecosystems globally offering software as a service (SAAS). The insurance industry needs to understand who is liable when there is an ecosystem breach and how this impacts the claim reserve. An example is a cyber-attack class that exploits the Internet Domain Naming Service (DNS) functionality for webservices (known technically as a "subdomain takeover") which causes subsequent defacement of websites and exposes vulnerabilities. Cloud service providers do not have a solution to this problem, hence the need to leverage integrity to protect customers and provide risk transfer capability.

Many organizations and regulators have been reluctant to embrace cloud migration and services due to cyber security, perceived loss of control over their Intellectual Property (IP) and data plus lack of situational awareness into where that data is and, how it is being used or ingested. Also there is a need to understand information rules that govern their critical digital assets. All these concerns are well founded without cyber integrity.

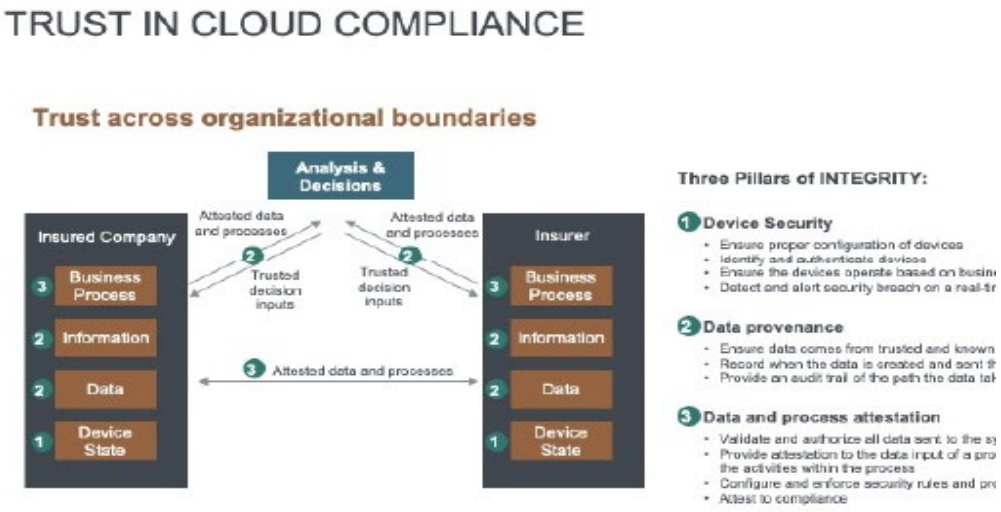
By independently, mathematically, proving integrity, definitive accountability is realized and evidence recovered from service providers and enterprises, provide truth to identify liability in the event of compromise across the cloud. From this new risk transfer solutions and new investible digital assets can arise with financial and societal benefit.

The result is monitoring and tamper detection of the network and proving an audit trail for data from creation to destruction that can never be erased in cyber space. This means underwriters and customers can trace data provenance from a clean slate network. This basic level of instrumentation can now provide proof of data creation, authenticity (is it the original?), and identity plus who accessed the data in its lifetime. It must work at the scales required for cloud computing, with evidence portable across all borders. This has big implications when addressing business interruption and IP theft insurance to know this baseline position. The data owner has the responsibility to ensure the original has data accuracy.

The Cloud Security Alliance (CSA)[x] point out that knowing who is liable in a breach is a challenge with shared responsibility between vendor and customer. This becomes the siren call of "we are all using best practices" which is trust not truth. It is misconception that the cloud

outsources the cyber liability risk so the onus is on the customers to invest in integrity as they are the owners of the data. Caveat Emptor.

For multinationals, outsourcing business trust to the largely unregulated cloud service provider industry (regardless of the contract guarantee) ultimately belies the belief in the constraints of the providers trusted insiders (and indeed any government) interactions with the data, as well as the integrity of purported technical security controls, to be in full abeyance of best practices and integrity of associated policies and processes. Moving to real time cloud regulation would help to address these issues. With integrity guarantees, true cyber security and relevant risk transfer for an organization is possible as in the diagram below.



IMPORTANCE OF THE ESTONIAN MODEL TO INSURERS

Estonia, a EU member and digital nation, is a country that embraced integrity from the ground up after a 2007 state sponsored cyber-attack. They applied cyber integrity to the INTERNET, while importantly preserving privacy. Their citizen identity management systems are backstopped by data tagging, generation and monitoring. Every critical security function, audit record, and critical data repository imparts evidence with continuous monitoring to ensure tamper detection, and resilience without reliance on stored secrets or human trust anchors. They have achieved mutual auditability between state, citizen, and participating private sector. This model is scalable and adoption to other countries is down only to political will. Importantly here it offers an insight to the insurance industry how integrity will shape the future of cyber risk. The integrity instrumentation is designed to afford the context of time. It is mathematically impossible to manipulate data generated in the past without the integrity of the data changing. Change detection of these assets and the ability to mutually audit the interaction is at the foundation of the ability for the Estonian government, private sector, and citizens to trust their data and verify it.

Cyber security is a triad of privacy (confidentiality), data integrity and accessibility (perimeter). GDPR regulations plus data scandals have brought the issue of digital privacy into the public eye and regulations, however, violating the integrity of data is even more dangerous, threatening lives and critical infrastructure essential to the functioning of society. In line with the theme of this paper, transparent truth, not trust, is the Estonian way. Significant friction is introduced to those attempting to lie, cover their tracks or change the evidence of an event in the past. The architecture and integrity technologies preserve the historical provenance of all interactions and indeed serves to preserve Estonian history electronically for the long term and imparts a gold standard for the insurance industry. Every cyber underwriter should visit Estonia.

CYBER INTEGRITY WILL DRIVE CYBER INSURANCE

Getting a single version of the truth by snapshot in real time at scale for all the machines connected to the network is game changer for insurers. With time from data compromise to discovery currently in months or years this identifies and flags changes to help mitigate or in some cases prevent cyber risk The reduced time to detection and granular, trusted, mathematically proven, near or real time data will have a significant shift effect on the current cyber insurance landscape. The importance of frequency and severity of cyber risk of future losses over a time horizon aggregates the loss and the detection will also mitigates

accumulation risk. For the insurance industry this is an unambiguous objective proof of breach and is an enhanced component of both existing indemnity based cyber coverage and capital market structures. There is huge protection gap or new premium that could be generated but does not currently exist because the integrity has not been applied. This has important implications on critical infrastructure on power grids, manufacturing, smart cities, supply chains and transportation. This will also pave the way to better capital market solutions, effective captive entities housing the cyber risk and private public partnerships. Many have stated that cyber could be an uninsurable risk or only possible if backstopped with government programs and integrity can counter these arguments.

With cyber integrity the underwriter is offered an interesting new range of information that can be applied in underwriting cyber risk.

1. Actual risk data giving rise to cyber event frequency proxied through real historical incidence of data tampering as opposed to "expected" or "forecasted" threat intelligence offered by physical breach sources. This would help to counter any lack of trust in cyber modelling.

2. Immediate detection / alert which enables prompt investigation and reducing the time from compromise to detection which can be as much as 500 days or more in some geographic areas.

3. Prevention especially for cloud computing where changes in configuration or risk profiles can be detected and corrected.

This widely witnessed evidence unlocks a new premium revenue stream by bundling operational assurance of cyber integrity into a suite of problem solving solutions for financial assurance and risk transfer. To the risk industry practitioner this can be a mix of indemnity, parametric, capital market (ILS), captives and hybrid offerings based on data driven evidence underwriting. Most existing cyber insurance is based on perimeter and confidentiality (privacy and encryption). A paper was released by EY in 2014[xi] addressing data integrity but very few, if any, contracts today have embedded robust cyber integrity into the policy wordings or covers.

The following insurance innovations are developing, via the Insure-Tech community or by the industry, based on cyber integrity.

1. Data Compromise Contingency Business Interruption (CBI)
2. Intellectual Property Theft
3. Telematic Transportation (autonomous) Liability Insurance
4. Cloud Computing ILS Vehicles
5. Cyber Captive Offerings
6. Parametric Cyber Offerings
7. Supply Chain Data Provenance Cover
8. Healthcare / Pharma Outcome Based Covers
9. IOT (Internet of Things) Insurance – extended warranty
10. Cyber Reputational Risk Offerings.
11. Plus more…

FINANCIAL ASSURANCE MEETS OPERATIONAL ASSURANCE

The lowest execution risk in the "merchant's warranty" approach to implement "financial assurance" with the “operational assurance” as white label approach to the IOT device endpoints. The data integrity provider embeds a warranty premium on top of the merchant fee via first-party warranty offering, or 3rd party insurance offering. The insured would benefit -

1) Should something not work as advertised during licensing term, the client will either get a partial fee refund or free license extension to another term in what is basically a money back guarantee.

2) To get a "immediate detection" discount for deploying integrity from their existing cyber insurance provider which, for some multinationals could be a significant amount.

Corporate c-suite should take note that immediate detection significantly lowers the company cyber risk profile to an insurer and reduces reputational risk at the same time which results in regulatory fines, customer loss or stock market dip. By investing in data integrity the cost centre of cybersecurity will show tangible returns.

Contingent Business Interruption (CBI) covers mainly physical damage and data compromise cover cannot be offered unless cyber integrity is in place. As measurement can start from a clean state network it will be possible to identify and capture changes in the context of time so we can cover data compromise and non-physical damage in conjunction with contingent business interruption, a large loss ratio risk factor.

MACHINE INTEGRITY

We have discussed the need for data and process integrity but to get the robust cybersecurity required we also need to look at the integrity of the configuration of the machines themselves. Recent developments in his area have emerged from Verizon namely machine state integrity (MSI)[xii]. More understanding on producing structured data is required by underwriters in order to define new products addressing the need of the growing cyber market and to keep up with the risk. This is massively important for 5G networks and necessitates a MSI instrument that gathers data about a network and deployed resources by taking snapshots of an entire network in the cloud over time and then making them available to the insurer who will just store them until there is an incident when they can then be analysed with forensic techniques for subrogation and liability purposes. Currently the cloud provider has no liability and this is a huge expense and legal problem. This will give insurers a vision into the black boxes of industry as to what happened by permissioned sharing of data.

PARAMETRIC CYBER INTEGRITY OPPORTUNITIES

Over half the economic losses from natural catastrophes are uninsured and this is not a healthy, sustainable protection gap. If we do not innovate for the emerging cyber risk we will face a similar issue. Indemnity insurance requires complex rating algorithms and detailed policy wordings. This has been the source of recent issues where policies have entered claim disputes because of ambiguity in the wordings not to mention recent exclusions of silent cyber policies where a cyber claim could appear in other policy lines such as property and director and officer policies. The move to stand alone cyber insurance policies is an opportunity to embed cyber integrity into the product design as standardization for intangible assets similar to the fire and

burglar alarms in the tangible world. During the pandemic disputes have arisen over business interruption and non- physical damage across supply chains in respect to indemnifying loss.

In comparison the use of parametric insurance solutions offer a means to guarantee and trigger a direct cash payment after a qualifying event occurs based on a simple IF-THEN action. This would serve to protect against unpredictable but potentially devastating risks that are not possible with traditional insurance products that indemnify for an actual loss sustained. The correct design of the data triggers is paramount to avoid basis risk where a contract could fail to pay when qualified or pay-out when not. For cyber some parametric covers may be deemed too small to cover the actual losses but in some cases the pay-out could be larger than actual losses incurred if the risk is triggered and the loss amount lower than the agreed expected loss. This approach can be taken to protect many situations such as loss retail business, reputational risk on social media, flight delay scenarios, hotel drop in occupancy rates, extreme weather and the cyber breaches as discussed below. There is a umbilical cord here to cyber integrity, utilising smart contracts, as we can meaningfully connect a given trusted data set to parametric insurance whether generated from machine integrity as described or from nano satellites, autonomous cars, healthcare technology, manufacturing, utilities or other sources.

Customers will use integrity to tag their most vulnerable nodes of digital and physical infrastructure (such as industrial control systems) of immediate interest to them from a cyber security standpoint and for which they want insurance cover. Standard verification features are then used to monitor assets for early warning detection, configuration snapshots in time and data tampering, all of which could be part of the trigger design.

This could be mitigation against active exploit, zero day trust, ransomware or other attacks. Underwriters can agree verification frequency with the customer as a pre-condition which could then lead to a proof of breach during the coverage period. This would be further verified by independent calculation agent to trigger the claims pay-out under the policy.

Using independent and objective trusted data for quick settlement of cyber insurance contract claims will turn many potential long tail liability claims into short term by creation of broad and bespoke contracts. This leads to a reduction of digital fraud, legal expenses, lower expense ratios and more accurate identification of liability in a multi-party, multi-location situation. The rich real time datasets generated will make this product approach more accessible over indemnity solutions. The time, labour and investigative expenses to research data breach to say nothing of the damage that could be inflicted to industrial control or software system & data between breach and its resolution are compensable damages by this innovative cyber insurance policy in a manner agreed upon between customer and insurer.

This ability to quantify risk of an email outage, or website/network / cloud being down or infrastructure breach can lead to a simple, relevant binary parametric cyber solution rooted in integrity goes a long way to unlock new approaches. Multi-party arrangements between broker, capital providers, insurers and integrity vendors would license the digital cyber asset across the distribution channel. Information can be shared with regulators that there is serious interest from hedge and pension fund(s), broker(s) and protection buyer(s) in arranging an innovative insurance/ cyber risk-transfer transaction via insurance linked securities (ILS) that will include an integrity standard as part of the deal structure.

Regulators do not need to get hung up on parametric aspects of the deal. If they are familiar with an indemnity transaction, integrating a tiny indemnity trigger as done in insurance linked warranty (ILW) will satisfy their regulatory requirements. Certainly, a client should not care

whether the protection contract is in the form of insurance, derivative, or service warranty, especially if investors fully collateralize the limit.

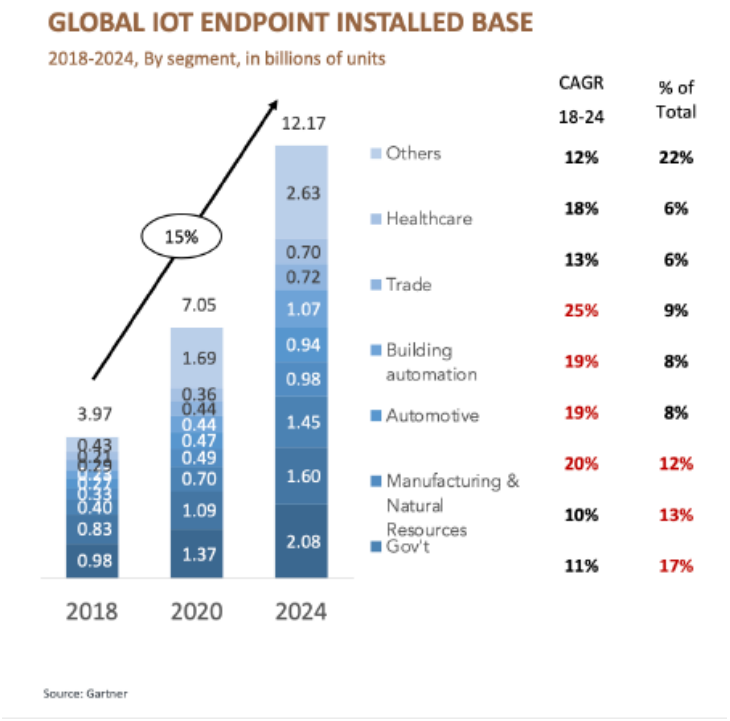
PARAMETRIC EXAMPLE

We need to illustrate how the limit of these integrity triggered deals is set and priced for a particular client and how is basis risk handled. Immutable data by definition will greatly reduce basis risk but there will always be an element of basis risk which is why there are deductibles in indemnity insurance. The limit is set based on client's particular circumstances. If we view our cloud problem of website defacement in the context of "digital business interruption", a client should have an idea of both direct costs of getting their website back online as well as of indirect costs of lost commerce, business interruption due to a website being down.

The sum of direct and indirect costs of website defacement would likely approximate the limit or sum insured that the client would want to recover in the event of such an event. In order to calculate premium protection sellers would need to establish empirical frequency of the website defacement event (or future likelihood based on such frequency) which would be proxied by measurable integrity solutions.

An example would be if integrity tagging shows that over the past 6 months there were 10 critical digital asset types tagged and one of them was compromised, then the conclusion is that the empirical frequency of defacement is around 10%, and therefore if the client wanted to recover $10,000 in the event of next such defacement over, say, the following 6 months, than, roughly, the client would pay 10% of the recovery limit, or $1,000 in premium for such a protection. Claims on such an event are essential to test the structure, prove its value and reinforce integrity for cyber risk-transfer as a quickly paying alternative to cyber indemnity pools but not a substitute. This is bespoke case by case. When one is basing cyber insurance on assets being tagged in near or real time then this insurance can be done as long as the distinction is made between authorised changes and unauthorised breach changes which would be tracked in an immutable blockchain audit trail. Building a pause into the parametric trigger would enable the insurer to validate the whether the change was unauthorised.

This spawns new applications for marine, aviation, healthcare, telecommunications, motor telematics, manufacturing , supply chain, all benefiting from cyber insurance based on integrity and data driven underwriting attached to cyber , business interruption, IP, reputational risk and liability lines based on global IOT endpoint expansion.



IOT installations are projected to grow significantly, as shown here, motivated by increased visibility and automation which are the business drivers to create more scalable operations such as predictive customer maintenance, remote operations and smart manufacturing. Customers are now demanding the ability to measure, automate and analyse data in proportion with their insurance cover. IOT insurance gateways, the subject of a follow up paper, will allow integrity of data at device source to be embedded and rated for protection and measurement.

CYBER INTEGRITY POST PANDEMIC WORLD

Given this paper was written at the time of the 2020 pandemic no one can deny the fact that the status quo in the areas of supply chain, government, healthcare and insurance have failed to perform adequately and this has accelerated business innovation driven by exponential technology such as blockchain, AI, IOT, mobility, big data and smart contracts. These technologies were already used on the side lines of these sectors but now we see the potential of mainstream adoption and increased digitisation. Many cyber-attacks occur during diversions and the pandemic will lower the cyber guard of individuals and corporations alike. The insurance industry offered pandemic cover to large corporations prior to the event but nobody bought, pandemic bonds were also in place, and although they triggered, were not adequate. Catastrophe cover for a global cyber-attack now if occurred now would also be inadequate. So there is need for new assets and risk transfer to be in place before the next “disease X“ appears for example and get it in place while memories are fresh.

HEALTHCARE

The global healthcare sector must plan a correlated cyber risk element to protect the privacy and integrity of healthcare data. Such offering would address one of the biggest, boardroom level pain points for public and private entities in the global healthcare / pharmaceutical industries in our digital age, namely the security of their patients' data and that of their own IP,

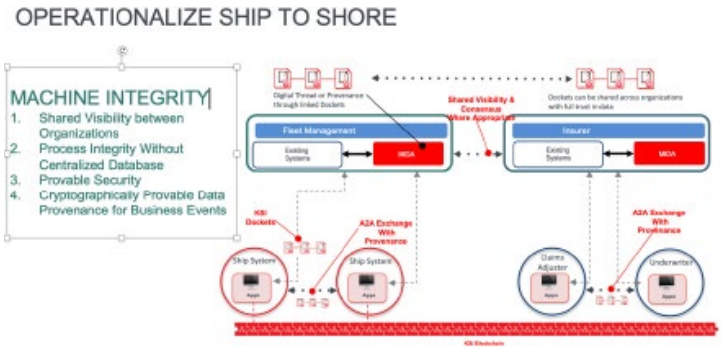
to say nothing of the financial implications from breaches thereof. The integrity solution in this paper would be part of the process for the transparency, credibility and relevance of the triggering mechanism for the underlying risk exposure. This would be applied to performance outcome-based medicine and pharma exposures plus effectively serving as a contract trigger in an integrity enabled parametric pharma supply-chain risk-transfer contract. The issue of integrity of manufacturing process and its underlying data in pharma industry is another great avenue to apply our financial assurance offering to, given that pharma companies around the world are well-known to warehouse most of their risk on their own balance sheets (via captives) owing to unavailable / unaffordable insurance coverage in the commercial insurance market.

SUPPLY CHAIN

In the digital world supply chains are subject to compromise as the automation of the process opens up gaps where compromise of data and process integrity causes counterfeit and unauthorised recycled products to enter the supply chain and the authenticity and identity of the buyer and the seller can be called into question. The world has been witness to the complications and fraud that have been associated with the PPE distribution in the world in the wake of the pandemic. Applying cyber integrity to the whole length of the supply chain will create an end to end data provenance that can be verified with appropriate risk transfer.

MARITIME

The diagram, courtesy of Guardtime[xiii] below connects a ship instrumentation to integrity on shore to provide end to end data provenance as a ship moves through the water. In 2021 regulation will be applied to the shipping industry to enforce cyber mitigation and proof will be required by inspection to prove that it has been installed. The Guardtime KSI, keyless data integrity technology shown in the diagram, ensures that insurers will know to what extent the insured has mitigated the cyber risk. This same technology can be applied for public transportation, motor, aviation and smart cities. This will prove compliance to security policy thus removing accidental configuration from the process.



CONCLUSIONS

For insurance providers and their customers to benefit from cyber integrity they must recommend a virtuous circle of two mutually reinforcing layers of operational and financial assurance, combining to improve operational cyber resiliency through real-time alerts, absolutely crucial when considering the lags between compromise and detection. This

addresses the kill chain of cybersecurity and makes damage mitigation obligatory with better tools. Governments plus military, defence and telecommunication industries have deployed this approach for sometime.

Cyber integrity is the foundational instrumentation required to provide detection mechanisms and provides a new dawn for cyber insurance. Integrity instrumentation allows you fundamentally the ability to tag, track, and locate assets and events in cyberspace.

With this ability, truth becomes widely witnessed evidence without disclosing the content of the underlying data (ensuring privacy), the evidence is portable and independently verifiable across infrastructures, and travels with the data. Cyber integrity means that customers, auditors, data-brokers, and investigators can independently answer the critical question:

"What changed, what was eliminated, when did it occur, and what was responsible"

So for the insurance industry weighing and insuring cyber risks how can underwriters achieve truth to calculate in real-time the integrity of the responsible interfaces, applications, and service layers responsible for the data. For the insurance industry to back these assets, they should require that evidence of integrity in the organizations data and information rules governing the systems that manage that data is a must and should be independently verifiable without having to trust the organization hosting those assets. There must be transparency and accountability if indemnification is to be identified when a mishap or compromise occurs i.e. who was responsible and can the evidence be irrefutably proven in a court? How can you possibly trust the service provider to say, 'it's not our fault, we are not liable', when there is no evidence to confirm or contradict the statement and what little evidence that remains might be presented is entirely shaped from the perspective of that service provider. Integrity instrumentation and its requirement is essential.

Auditors provide little confidence as they also rely on the same evidence, which can be erased without attribution by the responsible party. Requiring data integrity instrumentation in this way can bring accountability to the service provider by highlighting the complete chain-of-custody and digital provenance of service provider interactions, which in turn then identifies the responsibility and indemnification for compromises, tamper, malicious insider activities, or misconfiguration.

Cyber integrity proof affords the consumer, service provider, insurer or data broker to finally independently trust the provenance and integrity of any network interactions, as well as the digital assets they are managing and/or consuming. This provides a better solution to at scale in the cloud to identify malicious insider behaviours and/or asymmetric threats that takes advantage of ever new implementation specific vulnerabilities not imagined by the software vendor or enterprise such as zero-day exploits, insider threat challenges, subversion by governments.

STANDARDISATION

Interoperability across complex ecosystems is vital as multiple security protocols and legacy systems exist. World Economic Forum identified a $1T gap due to 80% of telecommunication technology budgets are spent on legacy. Cyber integrity integrates with legacy and not just smart devices.

Industry is long overdue for data identity tagging where pieces of crown jewel data should be tagged as such so every host and network-based security enforcement points knows its sensitive and can then enforce security policies accordingly. It is important that the industry gets together and agreed upon more universal standard data-tagging schemas and protocols and embed them in every smart device across networks aware of their own rules. A lot of data breaches caused by unsecured IOT devices . Broader risk profiles are needed across whole enterprise with a need to get a consensus across all endpoints with different protocols. Control and awareness over technical assets and reduction in cost of compliance. What is needed is a standardised framework for measuring cyber risk plus a clear and objective contractual definition of what constitutes a cyber event.

The ideal world is mitigation before connecting devices and security by design and this will be achieved in the OEM space as manufacturers embed integrity into their products. If protection is not in place before devices are connected to networks then the insurance cover will not be adequate to safeguard the enterprise and assets within.

Underwriters want to see holistic security on a single version of the truth across the whole enterprise. We have to protect the whole value chain and life cycle of business.

The major reason for such unavailability and unaffordability of insurance, however, lies in a simple premise that you can't adequately price what you can't adequately measure. Cyber integrity in addition to serving a real-time detector operationally and misconfiguration prevention is also in a unique position of enabling quantification of cyber risk financially - an elusive challenge that, once solved, will transform the financial management of cyber risk globally in the reset of all sectors. Quantification of cyber risk has always been dogged by lack of historical data, the changing nature of the risk and access to granular real time data.

If you multiply that by the total addressable health / pharma / cyber risk market, and further assume repeat of such transactions every year (just as big corporates renew their corporate insurance programs annually), it's not hard to appreciate the size of this potential new financial assurance revenue annuity for Investors and stakeholders.

NOTES AND REFERENCES

---

i. The author acknowledges his colleagues Alex Korb and Matthew Johnson for contribution to this paper. (https://www.ponemon.org)

ii. (https://www.ponemon.org)

iii. (https://www.oecd.org/daf/fin/insurance/enhancing-the-role-of-insurance-in-cyber-risk-management.htm)

iv. (https://www.swissre.com/institute/research/sigma-research/sigma-2017-01.html)

v. (https://gdpr-info.eu)

vi. (https://www.indexinsuranceforum.org/faq/what-basis-risk)

vii. (https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer)

viii. (https://www.weforum.org/reports/the-global-risks-report-2020)

ix. https://en.wikipedia.org/wiki/Whitfield_Diffie

x. (https://www.cloudsecurityalliance.org)

xi. (https://www.ey.com/Publication/vwLUAssets/EY_-_Insights_into_cyber_security_and_risk/$FILE/ey-cyber-insurance-thought-leadership.pdf)

xii. https://enterprise.verizon.com/products/security/advanced-threat-analytics-and-detection/machine-state-integrity/

xiii. https://guardtime.com

10.2020

David Piesse
CEO, DP88

About the Author:

David Piesse is CEO of a family office, DP88, specialising in InsurTech initiatives in Asia - www,DP88.com.hk. David has held numerous positions in a 40 year career including Global Insurance Lead for SUN Microsystems, Asia Pacific Chairman for Unirisx, United Nations Risk Management Consultant, Canadian government roles and staring career in Lloyds of London and associated market. David is an Asia Pacific specialist having lived in Asia 30 years with educational background at the British Computer Society and the Chartered Insurance Institute.