Mitigation and Resilience of Cyber Risk

David Piesse

2nd ASHK General Insurance & Data Analytics Seminar
Friday 7 October 2016
Businesses and the economy need a predictable and deterministic environment to grow, where risk can be quantified and managed alongside investment and return.

The World Economic Forum believes the lack of functioning cyber security threatens as much as USD 3 trillion of non-realized potential growth during this decade. Cost of cyber crime is currently $500 Billion a year.

If we are investing more but performing worse, something is fundamentally wrong with the approach we are taking as a society to cyber security.
Cyber Security: one of the biggest problems facing Asian Companies

24 Aug 2016
**Asian companies have world's worst cyber security says study**
“Many Asian organisations are badly defended against cyber-attacks, a year-long investigation by US security company Mandiant indicates. The median time between a breach and its discovery was 520 days, it says. That is three times the global average. Asia was also 80% more likely to be targeted by hackers than other parts of the world, the report said”.

26 Aug 2016
**Police check Taiwan ATM hacking suspects**
“The ATM heist, which was reported in Phuket, Surat Thani, Chumphon, Prachuap Khiri Khan, Phetchaburi and Bangkok, forced the state-run bank to close more than 3,000 ATMs, half of its total number of ATMs”...

29 Aug 2016
**SWIFT, the global banking system is (still) under attack.**
The messaging network that connects the world's banks, says it has identified new hacks targeting its members, and it is warning them to beef up security in the face of “ongoing attacks” cyber attacks on banks in Bangladesh, Vietnam, the Philippines and Ecuador in which malware was used to circumvent local security systems, and in some cases, steal money”.

20 March 2016
**The biggest threat in 2016?**
“According to research by the Business Continuity Institute...recently named cyber crime as the biggest threat to business in 2016, ahead of skills shortages and terrorist attacks”.
Time to compromise vs. time to discovery

Over the last decade:

• Time to compromise has decreased, 90% less than a day
• Time to discovery has remained flat, only 15% found in less than a day
• For insider threat, 69% of compromise detections take more than a day; 35% take weeks or more

Source: 2014 Verizon Data Breach Report
Cybersecurity is a trillion dollar plus risk and modern security solutions do not address the problem.

Cyber insurance is currently limited in many cases to entry cover, lower limits, non acceptance by insurers, frustration from risk managers and no wording cover for physical infrastructure damage caused by cyber breach. Not adequate.

With increased connectivity (e.g. connected car) there are no means to prove exactly what happened when. There is no equivalent of a photo in the digital world as there is in commercial fire line of business.

We need to provide mathematical certainty, an independent audit trail for all human and machine activity in digital society. This is the mitigation required.
MAJOR CONCERNS of INSURERS – OPERATIONAL RISK

- Breakdown of critical infrastructure and networks (power grids, nuclear power stations, transport systems, telecommunications, water supply, steel mills, maritime systems, and oil energy plants) leading to business interruption and economic loss. Use of smart devices M2M (machine to machine) must be well defined in the risk assessment process.

- Long term data corruption or integrity which can be disastrous if going on for a long period of time without detection having a similar effect as IBNR (Incurred But Not Reported) claims on an insurer’s balance sheet.

- Large scale cyber attacks on Fortune 500 companies and state sponsored attacks

- A massive incident of data fraud or theft for example in the healthcare sector.

- Increased digitization on a global scale opens new threats for compromise.

- Accumulation Risk across Multiple Policyholders
CYBER RISK RESILIENCE

• Mandatory regulation leading to fines is a temporary solution to cyber risk and RESILIENCE is the solution and proactive mechanism to enable organizations to prevent, resolve and recover from cyber issues in a fast manner also reducing reputational risk as part of the process.

• The blurring of territorial boundaries by the cloud and the threat to data integrity becomes a challenge to maintain and define the auditability of what had happened as any process is only as good as it’s weakest link

• The physical world used resilience and mitigation to look at the natural catastrophes. This is the equivalent in the digital world.
The Problem: Governance and Trust

End-to-end systems have no representation of veracity at the digital asset level.

1. How do I prove that vital data is authentic (original), reliable (tamper free) and from a credible source (known origin)?


3. How can I prove chain-of-custody and provenance for vital data moving through my systems?

Generally, “How do I trust my data, and how can I prove it?”
Problem: How to Validate Electronic Data?

- Inside the organization: validation based on procedure and trusted insiders
  - Explosion in cyber-espionage and enterprise data tampering
  - Cyber attackers increasingly good at hiding their tracks
  - Over 70% of fraud is conducted by insiders
  - Management, regulators, auditors, courts have no transparency

- Outside the organization: minimal validation
  - Most data needs to be taken at face value
  - Phishing, malware, electronic fraud
  - With emergence of Cloud computing outsiders become insiders
The Need for Mitigation to get Resilience

• All agree a mitigation plan is essential prior to notification and identification is required as to what has to be protected and what is at risk.

• New products to separate First Party Coverage limits (regulator costs, fines, business interruption) from Third Party Coverage Limits.

• The **PRIMARY** solution to potential data breach and beyond is risk mitigation, prevention and best practice security standards on data integrity. The **SECONDARY** solution then is the insurance and reinsurance market.

• This will lead to enterprise wide cyber cover, reduced legal reserving, subrogation control, precursor to cover, warranty for claim payment and supply chain risk mitigation.
Cyber Resilience as part of Cyber Risk Management

• Technology can offer now cyber mitigation – Keyless Signatures.

• Post breach trend rapidly moves to pre breach – looking beyond breach.

• Evidence is key to the process of recovery and claims, subrogation, loss and combined ratio improvement

• No one insurance company can take on the vertical CYBER and no reinsurer will spread the risk without knowledge of the risk.

• The insurers want the reinsurers to address this risk and start to spread the risk with appropriate reinsurance treaties.
The Estonia Story
Estonian scientists have built technology that allows the entire planet to verify EVERY event in cyberspace in such a way that the PRIVACY of each event is maintained but the integrity of events cannot be denied. These integrity technologies hold the promise to provide complete transparency – impossible for governments, corporations, or users to lie – everyone can verify the integrity of events independently from those presenting them.

What Estonia has implemented at the digital level is TRUST BUT VERIFY – independent verification of everything that happens in cyberspace.

You can’t be perfect at preventing crime, but you can be perfect at detecting crime’.
Estonia

- Regained independence from Soviet Union in 1991
- 100% Electronic Banking
- 100% Electronic Health Care
- Over 1000+ Online Government Services
- i-Voting

- Victim of a world's first State Sponsored Cyber attack in 2007
- Headquarters of NATO Cooperative Cyber Defense since 2008
ESTONIAN DIGITAL IDENTITY

• Estonia Created KSI (Keyless Signature Infrastructure)
• Every Government Service and Private Services are on the Card
• This includes insurance, Heathcare and Banking
• Only thing not on the Card is Marriage and Divorce
• KSI is Omnipotent in Estonia
Understanding Cyber Risk
Cybersecurity solution is based on continuous verification of the integrity state of Enterprise network, digital assets and data.

By collecting, analyzing, correlating and reporting this evidence one can build an integrity snapshot of the network and important digital repositories and archives.

Any unauthorized change in the integrity state represents an attack, whether internal or external, and can be detected with 100% certainty and accuracy.

Verifying that DATA in your network is not compromised Lowering your RISK

Security Operations Center (SOC)
Chain of Truth over Trust – A Key Shift for the Future

TRUTH IN NETWORKED SOCIETY

TRUTH IN YOUR BUSINESS

TRUTH IN YOUR DATA

TRUTH IN YOUR INFRASTRUCTURE

Internet-of-Things Security

Cybersecurity

Big Data Regulatory Compliance

Industrial Infrastructure Assurance
Data Security: The Blockchain Killer App

The cost of ineffective cybersecurity is estimated at 3 trillion USD by 2020.

Our thesis and contrarian view is that the root cause for ineffective cybersecurity is the **lack of integrity** of systems, networks, processes and data.

Confidentiality is what you get when your systems have integrity.

Currently insurance underwriting is done on confidentiality and availability. This needs to add data integrity and educate boards for the understanding of this risk.
Confidentiality
ID-card
Mobile-ID

Preventing the disclosure of information to unauthorized individuals or systems.

Making sure that the computing systems, the security controls, and the communication channels are functioning correctly.

Security Model

Maintaining and assuring the accuracy and consistency of systems and data.

Availability
X-road

Integrity
KSI
blockchain
Historical Reasons Why Integrity Was Not a Focus

Throughout the 1990s what mattered was confidentiality of data in motion – not the integrity of systems. With IOT, Cloud, mobile devices the **integrity** of systems and supply chains has come to the fore. PKI works for its original use case not for large scale system integrity.
### Why Does Integrity Matter?

<table>
<thead>
<tr>
<th>Integrity Breach</th>
<th>Confidentiality Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Your car</strong></td>
<td>Your braking system stops working</td>
</tr>
<tr>
<td><strong>Your flight</strong></td>
<td>Your plane’s instruments report that you are 1,000 feet lower than you actually are</td>
</tr>
<tr>
<td><strong>Your local power station</strong></td>
<td>Critical systems compromised leading to shutdown and catastrophic failure</td>
</tr>
<tr>
<td><strong>Your pacemaker</strong></td>
<td>Shutdown and death</td>
</tr>
<tr>
<td><strong>Your home</strong></td>
<td>Your security system is remotely disabled</td>
</tr>
</tbody>
</table>
Changing Business Needs Demands a New Security Model for Data Integrity

and why cyber Risk is definitely not a traditional IT issue

STRIVES FOR 100% PROTECTION BY BUILDING PERIMETERS

Our systems are secured!

REQUIRES 100% TRUST, DETECTION AND ASSURANCE TO REDUCE RISK

Our we legally and financially safe?

CIO / CSO / CTO

CEO / CFO / CRO
Cyber Risk Requires Business Executive Management

5 Key Questions CEOs Should Ask regarding Cyber Risk
1. What is current level and business impact of cyber risks to our company? What is our plan to address identified risks?
2. How is our executive leadership informed about the current level and business impact of cyber risks to our company?
3. How does our cyber security program apply industry standards and best practices?
4. How many and what types of cyber incidents do we detect in a normal week? What is the threshold for notifying our executive leadership?
5. How comprehensive is our cyber incident response plan? How often is the plan tested?

Cyber Risk is a Boardroom Responsibility and not a ‘voluntary program’
CURRENT CYBER UNDERWRITING

Privacy/Confidentiality

Intrusion Detection/Availability

CIA TRIAGE

Data Centric Integrity

80% of the security budget investment getting 20% of the benefit. Underwriting has to move to Data Integrity – move 50% budget.
How Data Security will pay for itself

if this was a $50M USD company a year

In 2012, Cyber Ins was $5K per $1M USD coverage – max $200M limit of coverage

• Privacy and perimeter only
• No data centric model considered
• Mega breaches happened and raised risks

Now, $50K per $1M USD – max $500M USD – with caveats

• Need mitigation resilience with KSI
• Need data centric integrity to prove a lower risk is tolerated

Data Integrity can be covered by the costs of reducing risk
Industrial Blockchain
Blockchain Primer

Append-only system of record shared across business network

Shared Ledger

Cryptography

Ensuring secure, authenticated & verifiable transactions

Consensus

Shared Contract

All parties agree to network verified transaction

Business terms embedded in transaction database & executed with transactions

Broader participation, lower cost, increased efficiency and fraud reduction.
Blockchain Principle

“Blockchain” is a distributed database that maintains a continuously growing list of data records, chained together against revision and tampering.

“Distributed consensus” is an agreement between different compute-nodes over what is a true or false record.

As every client has a copy of the blockchain it is impossible to manipulate information and cover up your tracks. The integrity and provenance of information systems can be mathematically proven.
Registering the electronic transactions in a **global insurance blockchain** makes transaction fraud impossible.

Verification of the transaction authenticity is instant and can be performed by anyone, anywhere.

Zero disclosure of information, all transaction related data remains confidential and is **never** entered into blockchain.
New Infrastructure
INTRODUCING KEYLESS SIGNATURE INFRASTRUCTURE - KSI
INDUSTRIAL BLOCKCHAIN AND LEDGER FOR MITIGATION

KSI signatures (hash functions), linked to the blockchain, enable the properties of data to be verified without the need for trusted third parties, keys or credentials that can be compromised.

Upon verification, KSI Signature allows to assert:

• Registration Time
• Registration Entity
• Data Integrity
Cyber Resilience with KSI®

INVENTORY
- Record digital assets in the KSI Blockchain by keyless signatures.
- Insurance inventory for digital assets
- Cyber Risk Assessment Service to determine which assets are signed

DETECT
- Continuously verify that the network is still free of compromise
- KSI-based real-time alert upon compromise
- Pre- and Post Observational Support

RESPOND
- Notify insurance provider that there has been a compromise
- Make real-time decisions from the KSI real-time integrity information identifying assets compromised with a response service.

RECOVER
- Fix the problem and then restore the network to the original state by resigning the detected assets.
- Automated processes for eDiscovery and Subrogation
What can KSI Address for Insurance Industry – Risk Management

Cryptographically verifiable long running transactions and contract certainty of assets from policy to claims.

- New Claims Settlement and Payments Processes
- Healthcare Record Protection
- Underwriting on data integrity as well as privacy
- Cyber Liability Solutions
- Health and Safety Data Exchange
- Reinsurance Operational Efficiency

But Insurers are also businesses with vulnerabilities, and production requirements for compliance and regulatory reporting and security.

- Fraud detection, prevention and expense ratio reduction
- Insider threat
- Regulatory archival – e-discovery
- Cloud and Big Data Provenance – IoT New Products
- Digital Identity – KYC/AML
- IP Theft New Products
- Dispute Resolution – less legal reserving – subrogation
- Claims Consortia run by the industry
KSI Ledger - What can it do for Insurance?

**Transactions:** are the main type of activity, and represent a transfer or payment of a premium/claim quantity of an insurance asset from one KSI Ledger Account to another, and represent a change in the claim on assets held at the Settlement company. Provide contract certainty.

**Assets:** can be defined by any permissioned user, they are insurance contracts represented by the hash value.

**Accounts:** represent an entity's balance of an Asset. An Account relates to one specific asset – multiple Accounts are needed for multiple Assets. Accounts for reserving, claims, premiums, reinsurance and endorsements.

**Issues:** Issues are the primary bridge for assets from the traditional insurance system to KSI Ledger and back. This aspect addresses the claims settlement system.
CONTRACT CERTAINTY WITH BLOCKCHAIN KSI APPROACH

Mitigate Risk
Minimize Capital
Reduce Loss

- Invest in holistic approach
- Granular, reliable data
- Straight-through with feedback loop

Customer instructions
Data Entry
Validation
Completion
Approval
Verification
Transaction
Posting

Typing errors, fraud
Oversight
Missing data
Rejects and rework
Inconsistencies
Failure, lateness
Incorrect details

$ Billion
Underpinning the Risk with the Risk Management Blockchain
Cryptographic Chain of Custody: Insurance

KSI can be used to create a chain of custody, establishing when, and who touched or modified data during each step in processing a transaction.

When claims payment processing data for example is saved to disk, KSI verification proves that the data has not been changed while it was vulnerable.
E-Discovery requires the ability to produce as widely witnessed evidence all potential data to discuss the status of the data from whence it came, has it been tampered with and when was it created. This means that all electronically stored insurance information needs to be stored for long periods – registers to SOLVENCY II/C-ROSS regimes.
New Insurance Products Enabled by KSI Blockchain

Goal is to allow new products to be created currently not possible pre blockchain and a warranty based on the properties of KSI in policy wordings and OEM.

1. IP THEFT type products detecting copying starting with a clean state network

2. IoT insurance products using software and digital supply chain warranties to big data lakes and repositories. Allows data provenance for health and safety data exchanges based on data collection from telematics, health devices and M2M environments.

3. Enhanced policies for cyber liability using KSI warranty in the policy wordings based on international standard. Allows for comprehensive cyber policy, with higher limits and lower loss ratios with easy options to spread the risk by risk transfer.

4. Allow new product to be created based on existing technologies by embedding of KSI. A good example would be KSI:Sharepoint for pharmaceutical clinical records. Better protection products for healthcare.
Snowden Would Never Have Been Able to Do What He Did if Data Logs Were Signed with KSI

Keyless Signature makes it impossible to lie
Governments and corporations and citizens get complete accountability and transparency as everything that happens can be independently verified
Pharmaceutical Clinical Trials

• The Administrator can configure the lists to which KSI is applied
• When KSI is applied to the list, each asset is automatically signed upon adding and upon update (new version)
• End users see the signature verification status next to a corresponding item
Big Data Regulatory Compliance: Data in Motion is Moving to Data at Rest – Needle in a Haystack Situation

1. **Know the 4W’s of Big Data**
   Know the who, what, where and when for your big data assets.

2. **Blockchain Backed**
   Built on industrial-scale blockchain technology for leading edge security.

3. **Immutable Audit Trail**
   Powered by a bullet-proof cryptographic audit trail designed for legal compliance.

Big Data Needs *veracity at scale* and Data Provenance
Big Data assets based on industrial-scale blockchain technology
Big Data Security
- Data Provenance

Insurance Industry Data Security Challenges -
Regulatory Compliance for the Insurance Industry continues to evolve for Legal, Big Data, Internet of Anything (IoAT) and Cyber Security.

As such, insurance companies need a foolproof way to prove veracity of data being stored in widely distributed data lakes like Hadoop and data in motion, the IoAT.
DIGITAL EVIDENCE IS LIKE LOOKING FOR A NEEDLE IN A HAYSTACK – Data in Motion Moves to Data At Rest.

ANSWER IS TO HAVE REAL TIME SITUATIONAL AWARENESS FOR EACH STALK OF HAY – DATA PROVENANCE IS KEY TO UNDERWRITING RISK
IoT Data Supply Chain Provenance

Internet of Anything

Capabilities
- Native Hadoop Integration
- Register at Ingestion
- Continuous Verification
- Indefinite Term Proofs
- Evidence Export
- Provenance Graph

Central Blockchain Service

Digital Fingerprint + Metadata

Apache Hadoop

GOVERNANCE

Legal Hold & Archive
- e-Discovery / Forensics
- Chain-of-Custody

Data Provenance at Scale for Data Lakes and Surrounding Data Ecosystem

Defensible End-to-End Lineage
Smart Cities Need Smart Grids and Meters

All metering data is signed to blockchain as it’s collected, inside the smart meter, enabling validation of all data at any point afterwards.
What do Enterprise CIOs need for Cloud Migration?

Q: What do CIOs need to move their mission critical processes to the cloud
A: “accountability, reliability, compliance, security, verifiability, auditability, acceptance of liability” etc.

They demand that there is a secure supply chain and that every step in that supply chain can be verified in real-time and when things go wrong it is possible to figure out what went wrong and that there is someone who can be held accountable.”

Today not a single cloud vendor can say this.
Cyberattack on Estonia stirs fear of 'virtual war'

By Steven Lee Myers
Published: Friday, May 18, 2007

MOSCOW — The computer attacks, apparently originating in Russia, first hit the Web site of Estonia’s prime minister on April 27, the day the country was mired in protest and violence. The president’s site went down, too, and soon so did those of other ministries in a wired country that touts its paperless government and likes to call itself E-stonia.
IOT Provenance, Integrity and Assurance

Benefits

- On-board, real-time verification of uploaded executable code makes it impossible to inject malware or otherwise tamper with authorized set of instructions.

- On-board, real-time signing of the collected sensor data provides complete tamper evident chain of custody from data capture to storage to long-term archiving.
Regulatory Issues
REGULATORY DISRUPTION – EX ANTE TO A PRIORI – REGULATORY TECHNOLOGY

(1) Maintaining the security of the premium, claims and reinsurance systems and status quo by deciding what kind of network is in the policyholder interest and what extent it should be decentralized.

(2) Encouraging the development of new technologies that have social and economic benefits even if they hurt the existing financial institutions.

(3) Given the volume of new entrants regulators worry about reliability and stability and how to apply legal frameworks for consumer protection. KSI will provide warranty for new technology and the cloud.
Insurance Consortia - Truth of Records Exposed

- Work with Common Standard Blockchain
- Proper Dispute Resolution on immutable data
- Transparency with the regulator before and after the claim.
- Clear Audit Trail and Improved Risk
Threat of legal action will force better cybersecurity practices.

90%

Agree that third-party software providers should be held liable when vulnerabilities are found in their software.

65%

Have begun or are planning to insert liability clauses into contracts with third-party providers.

Credit: Veracode / NYSE
RMS/AIR Launches New Data Standard for Managing Cyber Insurance

Cyber Exposure Data Schema provides open standard for insurance industry

Important for Machine to Machine (M2M)

NEWARK, Calif. – January 19, 2016 –
Cyber Group Risk
exposure leads to your aggregation of liabilities

Financial fines will be assessed based on a corporation's Gross Turnover:

- US 10% (now)
- EU 5% (2016)
- Asia emerging

Class Action Law Suites are becoming world wide

Your multination footprint is your cyber attack surface without boarders and risks the will involve all countries meaning your liabilities will increase.
Case Studies
cyberliability management

use case: connected car or ship

Benefits:

 › Real-time monitoring of the software and data uploaded to and / or executed on the connected vehicle.

 › Forensic traceability of data in case of disputes – the ability to pinpoint liability, independent proof of what happened when.

Network attack vectors:

-enterprise  oen  grid  web  roadside  home

✓ Application and SW tamper events are detected in real-time.

✓ ECU reporting of compromise.

✓ Roll-back of SW & configuration to known trusted state.

✓ Real-time SW verification.

✓ Real-time tamper detection.

✓ Real-time mitigation and integrity monitoring of functions.

Services:

-a/v content  telematics  diagnostics  adas  dsrc
Volvo CEO: We will accept all liability when our cars are in autonomous mode

But the head of Volvo warns that without broad federal guidelines, the U.S. is at risk of losing its leadership position in the development of self-driving cars.

Two questions loom over automakers and tech companies as they push forward with the development and testing of self-driving cars: “Who is responsible?” and “What are the rules?”

Volvo unveiled the IntelliSafe Auto Pilot interface in October 2015, which will allow drivers to switch in and out of autonomous mode.

Courtesy of Volvo Car Group
Critical Infrastructure: Telecom Core Networks

Real-time situational awareness and end-to-end provenance for critical infrastructure components

- Firmware
- Configuration
- Software
- Audit Compliance Logs
KSI to sign all payments, Infrastructure events, and regulated phone call data.
POS Equipment Firmware Integrity

Vulnerability

Unauthorized firmware used to steal customer data.

Solution: Data integrity for firmware

• Sign firmware
• Verify continuously and during transactions
• Enables use of less expensive third party hardware
• Shifts liability and costs from acquiring bank to retailer
• Verification can be done in hardware or software
Cost Saving on KYC/AML

Blockchain based AML/KYC process.

- Source of Funds
- Identity/Address of customer
- Authorized individuals/beneficiaries
- Investigation results

Immutable records covering key AML/KYC components

Data can be maintained in central repository, and access controlled by the applicant. Serves as a “fast-track” for compliance by providing the most recent, cryptographically verifiable evidence to support application processing.
Use Case: E-Healthcare in Estonia

Estonia has an integrated electronic health-care information system consisting of:

- Fully electronic medical records
- E-prescription system
- National Health Insurance Fund

KSI blockchain is employed throughout for a complete tamper evident chain of custody to independently trace who did what and when, as well as to combat insider fraud, verify preservation of privacy and ensure end-to-end accountability.
Use Case: E-Healthcare in Estonia
Teleradiology – Telemedicine Case Study

LOCAL DOCTOR IN USA

X-ray image

Diagnosis / report

OFFSHORE DIAGNOSTICS IN PHILIPPINES

80% DOCTORS
20% PATIENTS

80% DOCTORS
20% PATIENTS

URBAN
RURAL

Chile
Clinical Trial Data Lifecycle Model
Wrapping Up
Closing Loopholes

- It must be remembered that cyber risks grow with each technical innovation and this affects data integrity – corporations improve security 20% each year and the hackers improve 300% each year – do the maths.

- The more new solutions for privacy and availability tend to open more data integrity holes.

- Mitigation policies must adapt and evolve with technological innovation to keep Enterprise Wide cyber cover and risk management still in place and ahead of the threat.

- Cyber cover gap will continue to grow. Are capital markets and ILS the real solution over indemnity in time?
What is the Insurance Effect in 2017

• INSURETECH Solutions will reach the market.

• New and Increasing Data Breach events and resulting regulations will increase the adoption of cyber insurance and risk transfer reinsurance or otherwise.

• The amount of data is increasing exponentially so the insurers will have more big data and a need to understand the provenance of that data prior to analytics.

• The amount of smart devices is increasing and that will increase the need for insurance industry to understand the implications and wordings for the risk.

• Cyber Terrorism is on the increase and governments need to work with private industry to ensure backstop.
INSURETECH PLAYERS 2016
CONCLUSIONS AND OBSERVATIONS

- Developing a cyber risk management framework in line with resilience, actuarial modeling, revision of IT contracts within a new legal framework involves mitigation using technology to establish a digital chain of command across the whole holistic enterprise risk management framework and should be part of the whole process.

- Add basic questions on how to link cyber risk to the assessment process and service required in the assessment area by insurers, reinsurers and clients. Sign the crown jewels of data.

- How does the risk management process emulate cyber risk – is it understood at C-SUITE level - which tools, processes and control does a company have to mitigate cybersecurity – i.e. KSI.
So for this industry weighing and insuring cyber risks... how can you achieve truth to calculate in real-time the integrity of the applicable interfaces, applications, and service layers responsible for the data? For the insurance industry to back these assets, it should be required 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.