Institute
and Faculty
of Actuaries

Quantifying Cyber Risk Using Data Integrity as a Mitigation Strategy Presentation title

David Piesse – Chairman IIS Ambassador Program

CRO Guardtime

25 May 2017

Institute
and Faculty
of Actuaries

Update on Cyber Risk

25 May 2017

guardtime

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”.

BBC NEWS

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”.

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”.

SWIFT

CNN

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”...

Bangkok Post

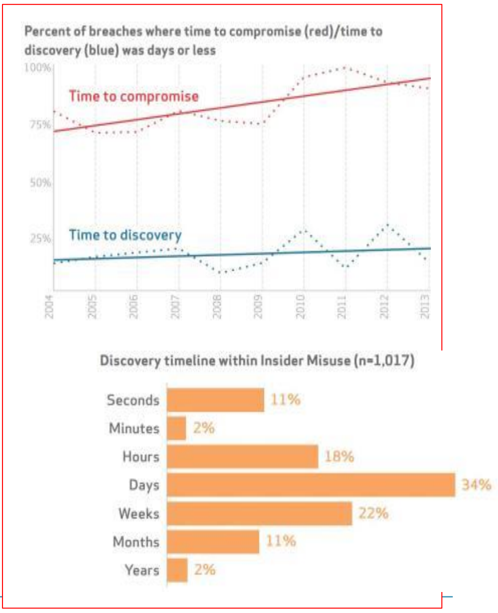
3

Time to compromise vs. time to discovery

Over the last decade:

- Time to compromise has decreased, 90% of attacks take less than one day
- Average time to discover a cyber attack in Asia is 1.5 years (520 days)
- For insider threats, 69% of compromise detections take more than a day; 35% take weeks or more

Source: Verizon Data Breach Report



guardtime

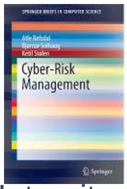
Cyber Security: problem of how to protect your data

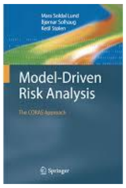
- □**Inside the organisation: validation based on procedure and trusted insiders**
  - ◉Explosion in cyber-espionage and enterprise data tampering
  - ◉Cyber attackers increasingly good at hiding their tracks
  - ◉Over 50% of fraud is conducted by insiders
  - ◉Management, regulators, auditors are not disclosing all attacks

- □**Outside the organisation: minimal validation**
  - ◉Most data is assumed to be real
  - ◉Phishing, malware, electronic fraud is increasing
  - ◉Cloud computing makes “outsiders” become “insiders”

- □**Over US$90 Billion in cyber security equipment, software and services**
- □**Over US$170 Billion in shifting physical paper around the world**

Challenges





- Digitization with Lack of Attention to Data Integrity
- Lack of Risk Mitigation Process in place
- Products are not what Risk Manager’s need
- Covers falling short of overall exposure
- Lack of claims data and future predictions
- Need to Improve Data Classification
- Multiple reinsurance layers required – government, capital market, captives and traditional reinsurance
- Regulatory Challenges

Cyber Risk Trends 2016-2017 Ist Qtr

Type		Description
DATA	↓	Physical loss, malicious breach – NOT DATA INTEGRITY
PRIVACY	↑	Un-authorised data collection – PII
NETWORK	↑	Network/Website Disruption
EMERGING RISKS	↑	Data Integrity, Email Compromise, Social Engineering

Ransomware events tripled in 2016 at least

Consumer Risk – Default Settings

- **A Message You Can Hug™**

mongoDB

Business Risk

YAHOO Merger and Acquisition Discount

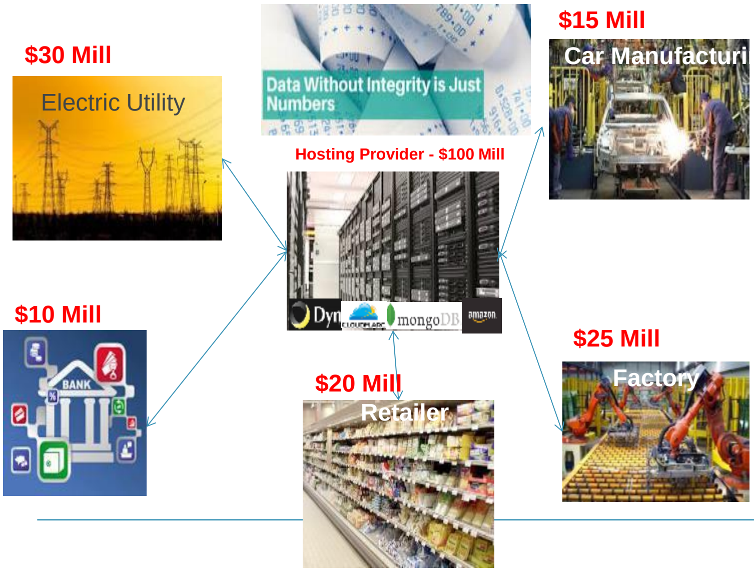
YAHOO!

verizon

RATINGS STILL DO NOT INCLUDE DATA INTEGRITY

BITSIGHT

Accumulation Risk – Regional Risk



$30 Mill

$15 Mill

Hosting Provider - $100 Mill

$10 Mill

$25 Mill

$20 Mill

Fortune 500 Accumulation Risk

Go Daddy®

65% F500 use for Domain Name Service

rackspace®
the #1 managed cloud company

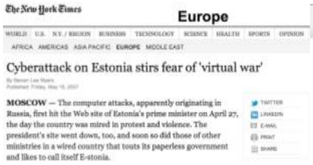
69% F500 use for Hosting

Akamai

77% F500 use for Content Delivery

Serious International Risks

Alleged and proven cyber attacks that could change the course of history.



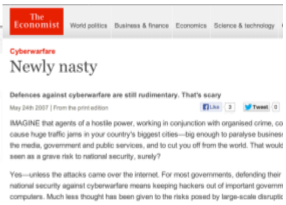
The New York Times
Europe

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINION
AFRICA AMERICAS ASIA PACIFIC EUROPE MIDDLE EAST

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.



The Economist
World politics Business & finance Economics Science & technology

Cyberwarfare

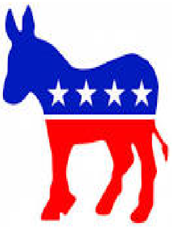
Newly nasty

Defences against cyberwarfare are still rudimentary. That's scary

May 24th 2007 | From the print edition

IMAGINE that agents of a hostile power, working in conjunction with organised crime, co
cause huge traffic jams in your country's biggest cities—big enough to paralyse busines
the media, government and public services, and to cut you off from the world. That woul
seen as a grave risk to national security, surely?

Yes—unless the attacks came over the internet. For most governments, defending their
national security against cyberwarfare means keeping hackers out of important governm
computers. Much less thought has been given to the risks posed by large-scale disruptio



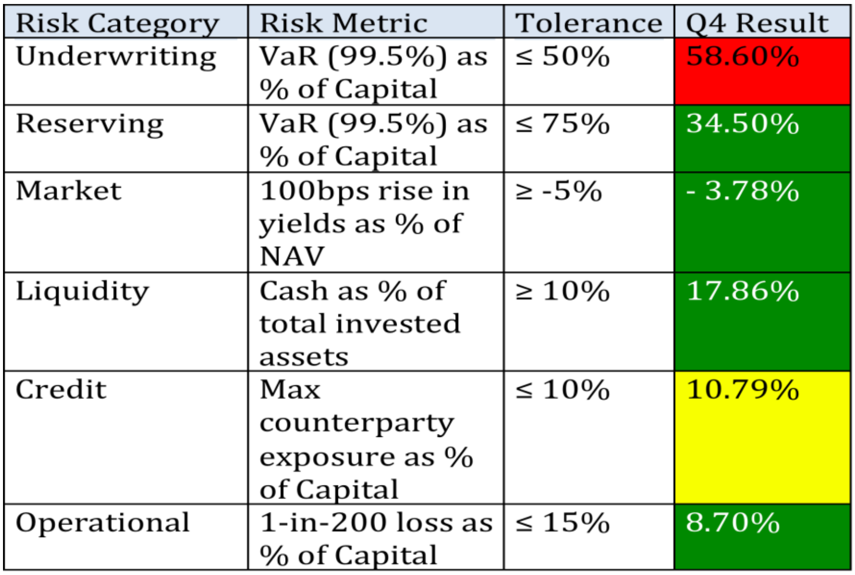
Institute
and Faculty
of Actuaries

Regulatory Issues

25 May 2017

The Issue at Hand

- Does Insurance Regulation Adequately Reflect Cyber Risk – answer no.
- A relatively new type of risk that is huge in magnitude and sits squarely in the operational risk area of the spectrum
- It is too big to leave in the operational risk all op risk bag and needs to be pulled out to the ORSA similar to cat risk.
- Huge lack of data has put up barriers. Incident data needs to be provided.
- Solvency II / RBC is not driving changes in models
- This is high frequency and high severity risk

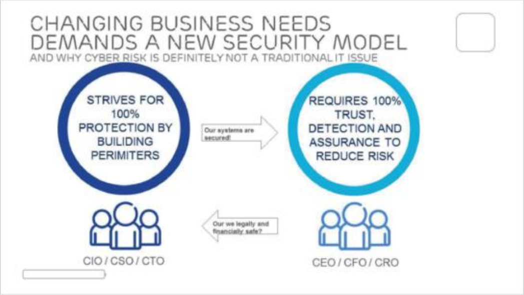


Risk Category	Risk Metric	Tolerance	Q4 Result
Underwriting	VaR (99.5%) as % of Capital	≤ 50%	🟥 58.60%
Reserving	VaR (99.5%) as % of Capital	≤ 75%	🟩 34.50%
Market	100bps rise in yields as % of NAV	≥ -5%	🟩 - 3.78%
Liquidity	Cash as % of total invested assets	≥ 10%	🟩 17.86%
Credit	Max counterparty exposure as % of Capital	≤ 10%	🟨 10.79%
Operational	1-in-200 loss as % of Capital	≤ 15%	🟩 8.70%

BOARDROOM REPORTING - ORSA

Management of Operational Cyber Risk

	Operational Cyber RISK	Underwriting Cyber Risk
Risk Management	Technical IT Security Improving Processes Education Cyber Risk Policies	Reinsurance Risk Transfer Insurance Pooling Screening Poliyholders
Responsibilty	Board and Compliance	Actuaries



CHANGING BUSINESS NEEDS DEMANDS A NEW SECURITY MODEL

AND WHY CYBER RISK IS DEFINITELY NOT A TRADITIONAL IT ISSUE

STRIVES FOR 100% PROTECTION BY BUILIDING PERIMITERS

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

Frequency and Severity

	Frequency	Severity
Drivers	Technology Cyber Crime Interconnected Systems Occurrence of Disasters	Mitigation in Place Crisis Management Dependencies on IT Sensitivity
Mitigation	Keyless Signature (KSI)	Cyber Risk Insurance

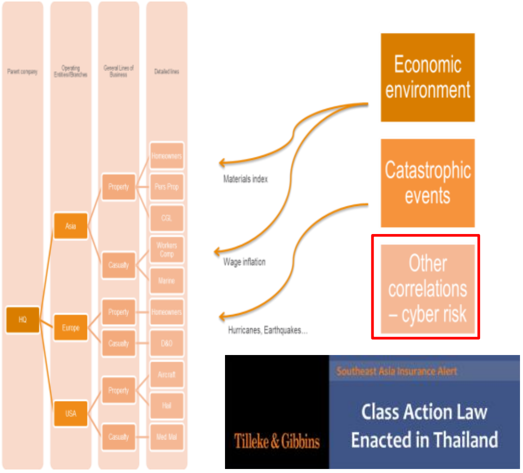
Estonia | NATO Cyber Security
The symbol of Estonian Cyber Defense League
CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Accumulated Cyber Attacks in the Cloud

Risk	Impact	Risk Mitigation
Many firms are leaner so are opting to use cloud computing, offshoring data and processes to third party firms. Critical functions outsourced include catastrophe modelling, actuarial analysis and compliance functions. 	A cyber attack could affect a firm's ability to process premiums and issue insurance contracts affecting cashflows and covers – particularly an issue for compulsory insurances. A cloud service provider concentration could become a second order risk if such providers were subject to multiple cyber-attacks causing a failure of services.	Ensure and monitor that third party firms provide the security and service that they are contracted to deliver. Constantly monitor data intergrity. Rectify breaches immediately to minimise security risks is paramount. Limit staff use of mobile devices to minimise damage to high risk critical areas of the infrastructure.

Cyber Group Risk

exposure leads to your aggregation of liabilities



- Financial fines will be assessed based on a corporations Gross Turnover:
  - US 10% (now)
  - EU 5% (2016)
  - Asia emerging
- Class Action Law Suites are becoming world wide
- Your multinational footprint is your **cyber attack surface** without boarders and risks the will involve all countries meaning your liabilities will increase

Institute
and Faculty
of Actuaries

Data Integrity and Mitigation

25 May 2017

guardtime

Cyber Risk Mitigation

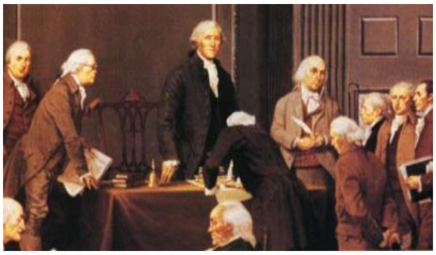
- Lack of understanding of complexity of risk especially data integrity
- Without data integrity there is no compete risk management framework
- Company runs the risk of customer identifying tampered data before the business
- Then increase in legal reserving and/or government fines
- Post breach action only mitigates further damage
- Pre breach action essential before risk transfer – early warning and monitoring
- BI is key to it all – financial health check, service provider checks, network infrastructure plus loss scenarios and modeling
- Rating for underwriters 400 – 700 range.

BITSIGHT

guardtime

The Problem: Governance and Trust

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

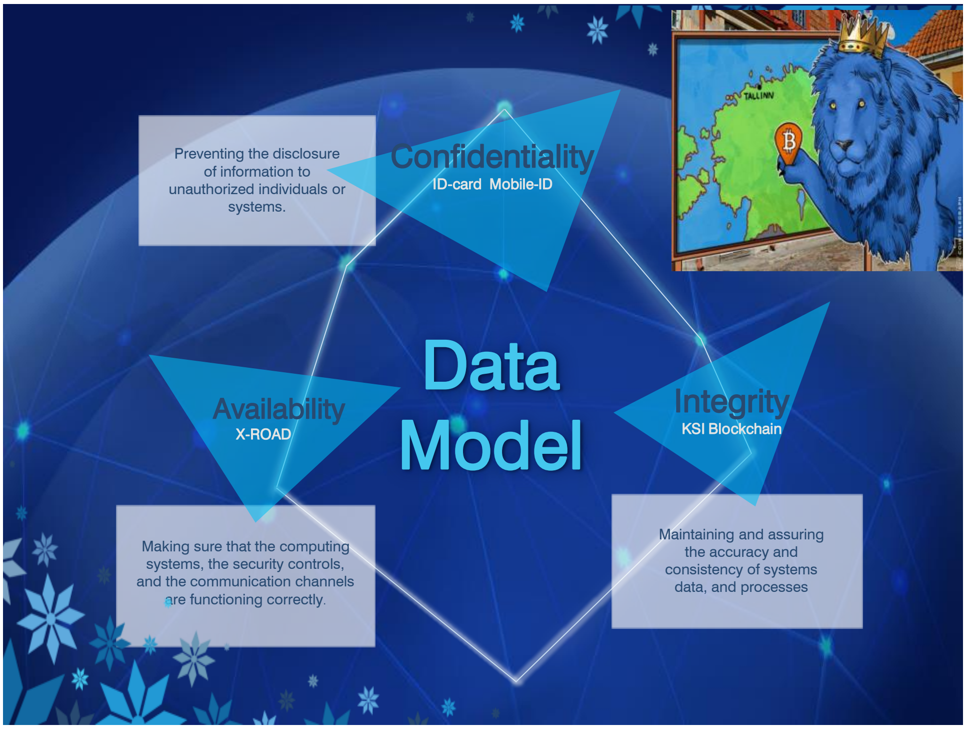


1. How do I prove that vital data is authentic (original), reliable (tamper free) and from a credible source (known origin)?

2. How do I eliminate manual processes and establish automated mechanisms to ensure long-term integrity in my digital supply chain.

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?”



Data Model

Confidentiality

ID-card Mobile-ID

Preventing the disclosure of information to unauthorized individuals or systems.

Availability

X-ROAD

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

Integrity

KSI Blockchain

Maintaining and assuring the accuracy and consistency of systems data, and processes

guardtime

Data Security: The Blockchain Killer App

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

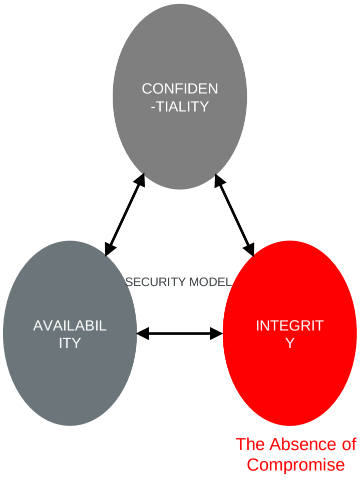
The cause for ineffective cybersecurity is the **lack of integrity** of systems, networks, processes and data.

What do we mean by integrity?

Knowing the data is real and has not be changed.

What does that mean?

Confidentiality is what you get when your systems have integrity.



Security spending not directed at Data Integrity

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

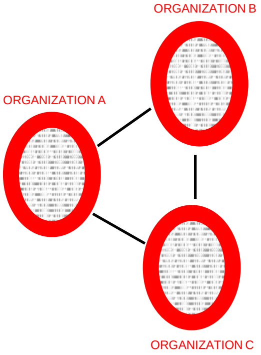
Cybersecurity

Big Data Regulatory Compliance

Industrial Infrastructure Assurance

guardtime

Using Secrets for Integrity is a BAD idea

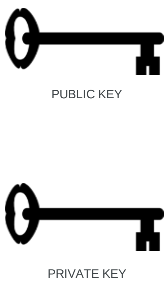


ORGANIZATION B

ORGANIZATION A

ORGANIZATION C

PKI



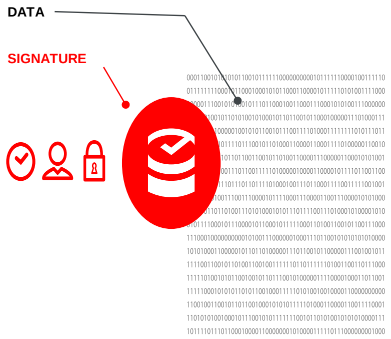
PUBLIC KEY

PRIVATE KEY

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.

guardtime

The Estonian Challenge: A New Form of Meta-Data



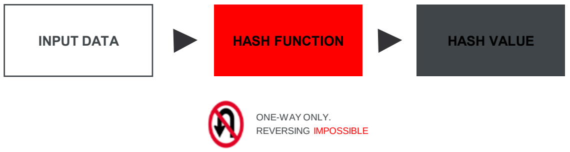
Based on the lessons learned from the 2007 state sponsored cyber-attacks Estonian scientists were set a challenge: design and building a tagging system for electronic data which could prove the time, integrity and identity (human or machine) without reliance on centralized trust authorities. Data must stay in the country.

guardtime

Cryptographic Hash Functions

Hash value is the digital fingerprint of the input data!

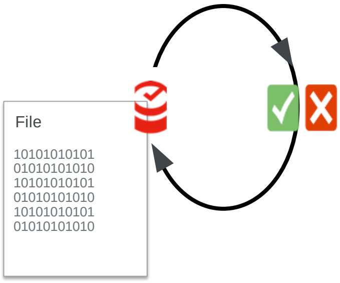
A hash function takes arbitrarily-sized data as input and generates a unique fixed-size bit sequence as output.



guardtime

Independent verification of the integrity of policy

Documents away from hosting entites.

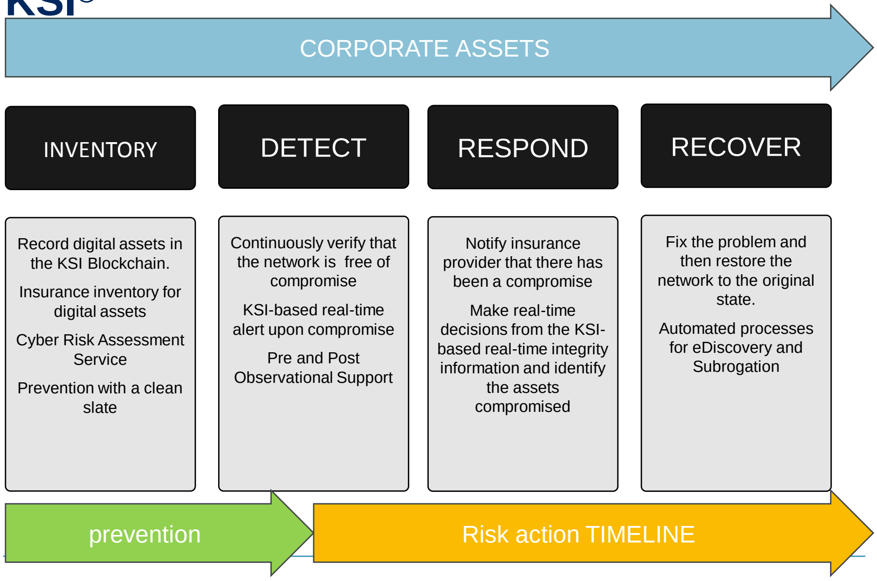


Signature anywhere, validated periodically

Whenever it is important to be aware
of any data breaches as early as possible

2
9

Cyber Mitigation and Resilience with KSI®


CORPORATE ASSETS

INVENTORY

Record digital assets in the KSI Blockchain.

Insurance inventory for digital assets

Cyber Risk Assessment Service

Prevention with a clean slate

DETECT

Continuously verify that the network is 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-based real-time integrity information and identify the assets compromised

RECOVER

Fix the problem and then restore the network to the original state.

Automated processes for eDiscovery and Subrogation

prevention

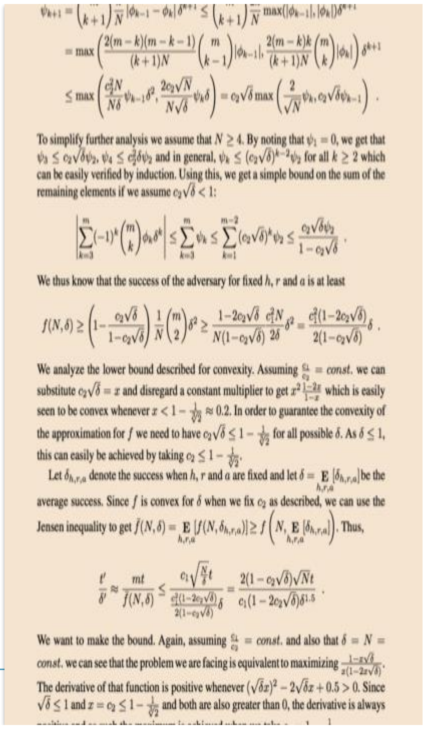
Risk action TIMELINE

guardtime

Formal Security Proof

Unlike with other blockchains, KSI has a formal peer reviewed security proof that it does exactly what is says it does.

As we have seen with the latest DAO attack, this is important



$$\psi_{k+1} = \binom{\;}{k+1}\frac{\;}{N}|\phi_{k-1}-\phi_k|\delta^{k+1} \le \binom{\;}{k+1}\frac{\;}{N}\max(|\phi_{k-1}|,|\phi_k|)\delta^{k+1}$$
$$= \max\left(\frac{2(m-k)(m-k-1)}{(k+1)N}\binom{m}{k-1}|\phi_{k-1}|, \frac{2(m-k)k}{(k+1)N}\binom{m}{k}|\phi_k|\right)\delta^{k+1}$$
$$\le \max\left(\frac{c_2^2 N}{N\delta}\psi_{k-1}\delta^2, \frac{2c_2\sqrt{N}}{N\sqrt{\delta}}\psi_k\delta\right) = c_2\sqrt{\delta}\max\left(\frac{2}{\sqrt{N}}\psi_k, c_2\sqrt{\delta}\psi_{k-1}\right) .$$

To simplify further analysis we assume that $N \ge 4$. By noting that $\psi_1 = 0$, we get that $\psi_3 \le c_2\sqrt{\delta}\psi_2$, $\psi_4 \le c_2^2\delta\psi_2$ and in general, $\psi_k \le (c_2\sqrt{\delta})^{k-2}\psi_2$ for all $k \ge 2$ which can be easily verified by induction. Using this, we get a simple bound on the sum of the remaining elements if we assume $c_2\sqrt{\delta} < 1$:

$$\left|\sum_{k=3}^{m}(-1)^k\binom{m}{k}\phi_k\delta^k\right| \le \sum_{k=3}^{m}\psi_k \le \sum_{k=1}^{m-2}(c_2\sqrt{\delta})^k\psi_2 \le \frac{c_2\sqrt{\delta}\psi_2}{1-c_2\sqrt{\delta}} .$$

We thus know that the success of the adversary for fixed h, r and a is at least

$$f(N,\delta) \ge \left(1-\frac{c_2\sqrt{\delta}}{1-c_2\sqrt{\delta}}\right)\frac{1}{N}\binom{m}{2}\delta^2 \ge \frac{1-2c_2\sqrt{\delta}}{N(1-c_2\sqrt{\delta})}\frac{c_1^2N}{2\delta}\delta^2 = \frac{c_1^2(1-2c_2\sqrt{\delta})}{2(1-c_2\sqrt{\delta})}\delta .$$

We analyze the lower bound described for convexity. Assuming $\frac{c_1}{c_2} = const.$ we can substitute $c_2\sqrt{\delta} = x$ and disregard a constant multiplier to get $x^2\frac{1-2x}{1-x}$ which is easily seen to be convex whenever $x < 1 - \frac{1}{\sqrt[3]{2}} \approx 0.2$. In order to guarantee the convexity of the approximation for f we need to have $c_2\sqrt{\delta} \le 1 - \frac{1}{\sqrt[3]{2}}$ for all possible δ. As $\delta \le 1$, this can easily be achieved by taking $c_2 \le 1 - \frac{1}{\sqrt[3]{2}}$.

Let $\delta_{h,r,a}$ denote the success when h, r and a are fixed and let $\delta = \mathop{\mathbf{E}}_{h,r,a}[\delta_{h,r,a}]$ be the average success. Since f is convex for δ when we fix c_2 as described, we can use the Jensen inequality to get $\bar{f}(N,\delta) = \mathop{\mathbf{E}}_{h,r,a}[f(N,\delta_{h,r,a})] \ge f\left(N, \mathop{\mathbf{E}}_{h,r,a}[\delta_{h,r,a}]\right)$. Thus,

$$\frac{t'}{\delta'} \approx \frac{mt}{\bar{f}(N,\delta)} \le \frac{c_1\sqrt{\frac{N}{\delta}}t}{\frac{c_1^2(1-2c_2\sqrt{\delta})}{2(1-c_2\sqrt{\delta})}\delta} = \frac{2(1-c_2\sqrt{\delta})\sqrt{N}t}{c_1(1-2c_2\sqrt{\delta})\delta^{1.5}} .$$

We want to make the bound. Again, assuming $\frac{c_1}{c_2} = const.$ and also that $\delta = N = const.$ we can see that the problem we are facing is equivalent to maximizing $\frac{1-x\sqrt{\delta}}{x(1-2x\sqrt{\delta})}$. The derivative of that function is positive whenever $(\sqrt{\delta}x)^2 - 2\sqrt{\delta}x + 0.5 > 0$. Since $\sqrt{\delta} \le 1$ and $x = c_2 \le 1 - \frac{1}{\sqrt[3]{2}}$ and both are also greater than 0, the derivative is always

Institute
and Faculty
of Actuaries

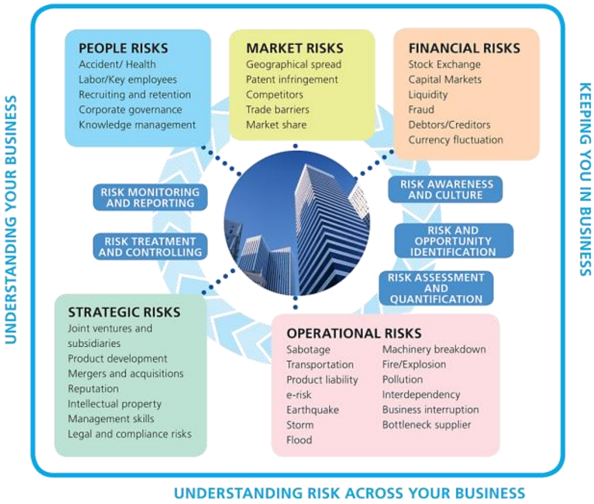
Risk Profiling and Risk Management

25 May 2017

Provide a “digital chain of command over events” is a major part of the resilience process and provide the truth making networks and the INTERNET attributable

- Truth can be measured – it means undeniable independent proof, which can be proven forensically in a court of law. Truth, not trust is essential for any network, enterprise, or data storage asset – it’s operation and interactions with the data being hosted should be able to be independently verified with forensic proof that holds up in a court of law. The organisations hosting the data are not involved in the verification process. Mutual auditability and non repudiation. The basis of who is liable.

Enterprise Risk Profiling



UNDERSTANDING YOUR BUSINESS

PEOPLE RISKS
Accident/ Health
Labor/Key employees
Recruiting and retention
Corporate governance
Knowledge management

MARKET RISKS
Geographical spread
Patent infringement
Competitors
Trade barriers
Market share

FINANCIAL RISKS
Stock Exchange
Capital Markets
Liquidity
Fraud
Debtors/Creditors
Currency fluctuation

RISK MONITORING AND REPORTING

RISK TREATMENT AND CONTROLLING

RISK AWARENESS AND CULTURE

RISK AND OPPORTUNITY IDENTIFICATION

RISK ASSESSMENT AND QUANTIFICATION

STRATEGIC RISKS
Joint ventures and subsidiaries
Product development
Mergers and acquisitions
Reputation
Intellectual property
Management skills
Legal and compliance risks

OPERATIONAL RISKS
Sabotage
Transportation
Product liability
e-risk
Earthquake
Storm
Flood
Machinery breakdown
Fire/Explosion
Pollution
Interdependency
Business interruption
Bottleneck supplier

KEEPING YOU IN BUSINESS

UNDERSTANDING RISK ACROSS YOUR BUSINESS

Carriers do guesswork and business leaders do Not understand the risk .

Need to move on from quantifying on records lost per breach

CYBER AND DATA RISK CURRENTLY BELOW THE RISK RADAR

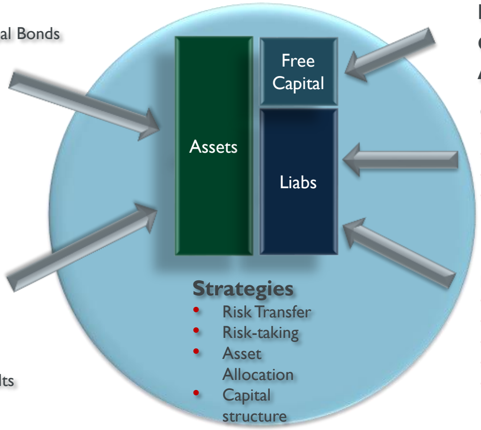
Capturing the Dynamics of Business within the overall Business Cycle

Economic Environment- Market Risk

- Inflation indices, Bond yields, Spreads, Stock indices, FX rates.

Asset Risk

- Treasury / Municipal Bonds
- Corporate Bonds
  - By sector
  - By rating
- Equities
  - By sector
- Real Estate
- Swaps
- Call / Put options
- Cash deposits



Free Capital

Assets

Liabs

Liquidity Risk

Group Risk

Asset Liability Mismatch

Operational Risk

- Privacy
- Fraud.
- Physical Infrastructure
- Catastrophe Risk

Strategies

- Risk Transfer
- Risk-taking
- Asset Allocation
- Capital structure
- Diversification

Product Liability Risk

- Reputational Risk
- Brand Assurance
- D&O/E&O
- Business Interruption
- IP Theft

Credit Risk

- Bond defaults
- Third Party Defaults
- Recoverables

DATA AND Cyber Risk is Buried in Product Liability and Operational Risk

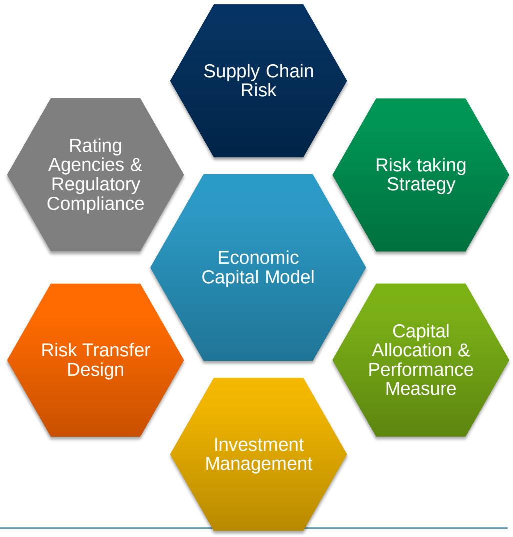
Uses of Internal Capital Model

Once built it can recalibrate to re-run on a regular basis

Modelling provides benefits for:

- Risk Transfer efficiency
- Risk taking strategy
- Communication with regulators
- Impact of M&As
- Capital adequacy of industry

Explore correlation and diversification of all kinds such as cyber risk



Supply Chain Risk

Rating Agencies & Regulatory Compliance

Risk taking Strategy

Economic Capital Model

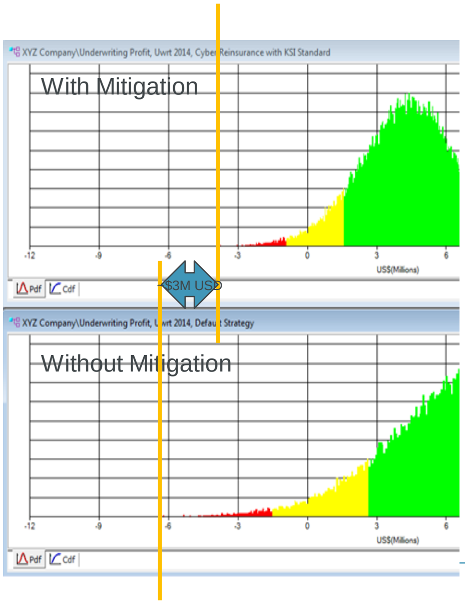
Risk Transfer Design

Capital Allocation & Performance Measure

Investment Management

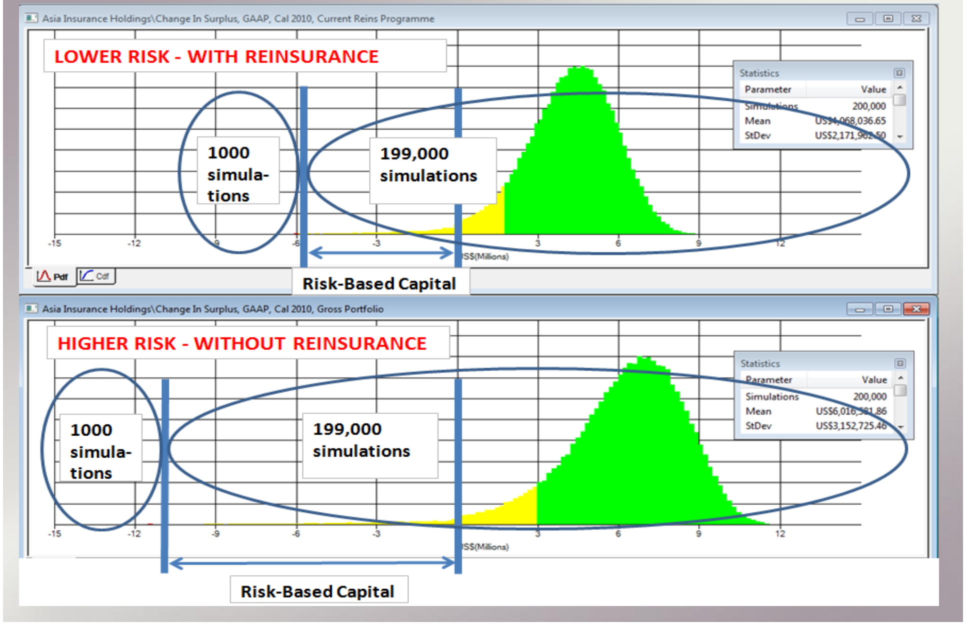
How Data Security will pay for itself

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

1 in 200 Worst Case Scenario = 99.5% chance of survival = 0.5% chance of bankruptcy – what for cyber is the question.


Asia Insurance Holdings\Change In Surplus, GAAP, Cal 2010, Current Reins Programme
LOWER RISK - WITH REINSURANCE
1000 simula-tions
199,000 simulations
-15
-12
-9
-6
-3
3
6
9
12
US$(Millions)
Pdf
Cdf
Risk-Based Capital
Asia Insurance Holdings\Change In Surplus, GAAP, Cal 2010, Gross Portfolio
HIGHER RISK - WITHOUT REINSURANCE
1000 simula-tions
199,000 simulations
-15
-12
-9
-6
-3
3
6
9
12
US$(Millions)
Risk-Based Capital

Statistics

Parameter	Value
Simulations	200,000
Mean	US$4,068,036.65
StDev	US$2,171,962.50

Statistics

Parameter	Value
Simulations	200,000
Mean	US$6,016,381.86
StDev	US$3,152,725.46

The Black Swan Event

- We all believe this will happen but do not know when and cannot put .a return period on it like earthquakes e.g. a 1 in 500 year event.
- Cyber is high frequency and right now relatively low severity but a larger correlated cyber-attack leading to black swan proportions which is long term corruption of data, physical infrastructure attack and a major fraud/forensics incident. Will rapidly change the profile.

Recent Development

LLOYD'S

Munich RE

RMS Risk Management Solutions

CATLIN

AIR WORLDWIDE

- Press Releases
- **RMS and AIR Launches New Data Standards 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 –

Alternate Capital Market Solution

- The capital markets will eventually enter the enterprise risk management modeling .
- This will be via ILS or insurance linked securities, pension funds, hedge funds, sidecars and others. .
- These can be in the form of bonds as in cat bond, **cyber indexes** and other vehicles.
- Discounted cash flow models will need to show different output to investors.

Also CAPTIVES

Data Requirements

- A loss database across all lines of business in insurance – D&O, E&O, General Liability and more.
- A cyber database consisting of 350,000 events with frequency, severity, cause and cost of breach. This is expect to double every 3 months.
- A technical database with network and digital asset information that can be used for rating.
- A taxonomy based on insurance event, litigation, penalties and fines, third party costs, response information, insider involvement and subrogation.
- A company database close to S&P Enterprise Information that holds corporate details of 20 Million companies.

ADVISEN Insurance Intelligence

CAMBRIDGE Judge Business School

INSURANCE INFORMATION INSTITUTE

NetDiligence®

Institute
and Faculty
of Actuaries

Identification and Data Ownership

25 May 2017

Benefits of Digitization

Easy Identifcation

e-Solutions simplify and benefit our lives.

- BLOCKCHAIN IDENTITFICATION IS KEY BUSINESS
- PROOF OF IDENTITY plus LONG TRAIL of IDENTITY (FB ID)
- DIGITAL IDENTITY MEANS YOU KNOW WHO OWNS THE DATA
- SENSITIVE DATA NOT STORED ON THE BLOCKCHAIN

Empowering in Estonia

Everything can be done online except for ?

- ONCE-ONLY PRINCIPLE
- NO LEGACY
- DIGITAL BY DEFAULT
- SINGLE POINT OF ENTRY
- USER FRIENDLINESS
- OMNI-CHANNEL
- SERVICES
- OPEN STANDARDS
- 24/7

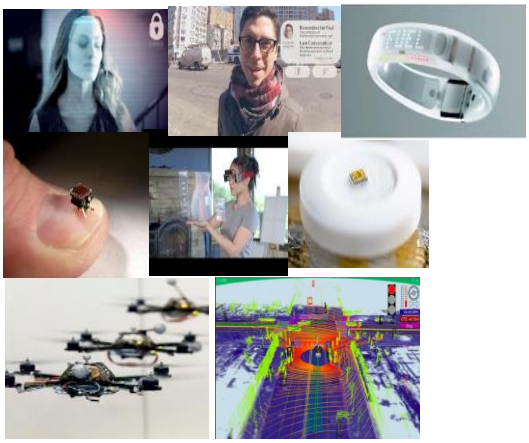
e-Residency

Become an e-Resident like 12 000 others

Over 650 new companies established in 1 year!

Internet of Things - Device Immersion

- **Devices need to be**
  - ***authenticated***
  - ***verified,***
  - ***permitted***
  - ***Governed***
  - ***trusted third party***
  - ***just like people***

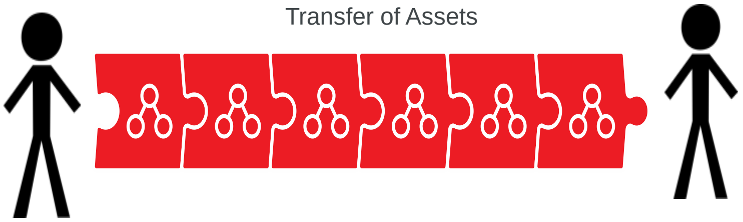


Cost Saving on KYC/AML

- Data Protection and Security
  - Permissioned Blockchains
  - Regulatory Compliance
  - Transaction trail for audit
  - Non repudiation and widely witnessed evidence
- Data can be maintained in blockchain 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.

BLOCKCHAIN MEETS AI/MACHINE LEARNING

Blockchain Transfer of Assets – no need for Middleman – Operational Efficiency



Transfer of Assets

Trusted Identity

Trusted Identity

guardtime

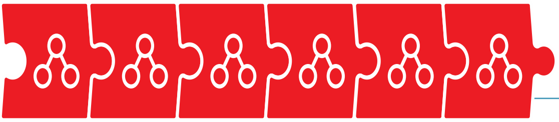
The CONSORTIUM

Consortiums

R3

- Streamline Business Processing
- Improved Policy Administration
- Faster Customer Payments
- New Investment Management
- Better Distribution of Proceeds
- Fraud Reduction
- Need Digital Identity Frameworks

B3i

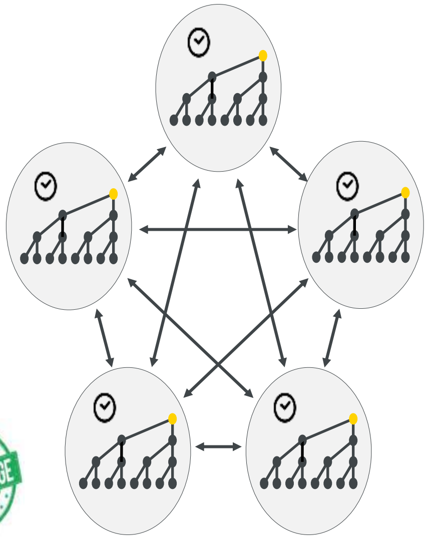


51

Regulatory Models with Blockchain

- How will industry consortiums interact with regulators ?
- Will regulators act as another node on the network so as to have
- permissioned access in real time to the ledger.
- Will a SUPER Regulator will be required as regional
- nodes are shared to review systemic risk.
- Global Regulation vs Regional Regulation via consortia.
- Leveled model where all regulators share a private ledger
- Cannot regulate a technology but the blockchain is a protocol spawning activities that can be regulated
- Right now there is no regulation for financial services outside of regulatory sandboxing
- There are existing laws related to smart contracts for commercial trade. KYC/AML, data privacy/breach

ARBITRAGE



guardtime

Big Data Legal Implications

Enabling Big Data Regulatory Compliance

Legal Hold

Chain of Custody

Long Term Archival

E-Discovery

Data Assurance

Forensic Readiness

Veracity at Scale for Data at Scale

Big Data Blockchain Concepts

100% Accountability

Data events are captured and record time, integrity of asset, and signer origin.

Immutable Ledger

Impossible for anyone to tamper with ledger and any data tampering can be easily detected.

Universal Time Source

Time is an inherent property of the system so events can be unified across distributed systems.

Decentralized Consensus

Ability for auditors, law enforcement, or third parties to independently verify asset veracity.

Keyless Signature Infrastructure

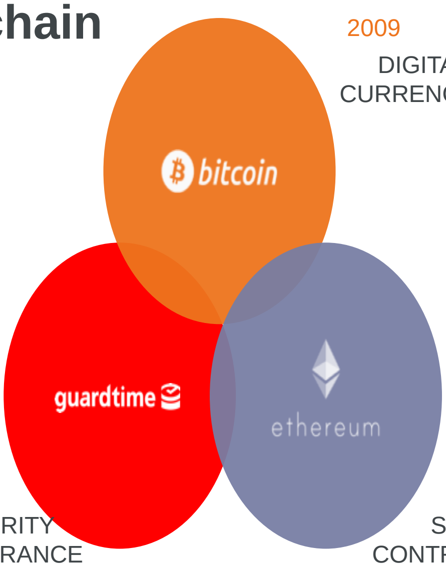
53

guardtime

Intended Blockchain Use Cases

Taking a technology designed for Cryptocurrency and applying it to Smart Cities can never work.

Estonia's KSI Blockchain is an optimized protocol for massive scale data management and cybersecurity.



2009
DIGITAL
CURRENCY

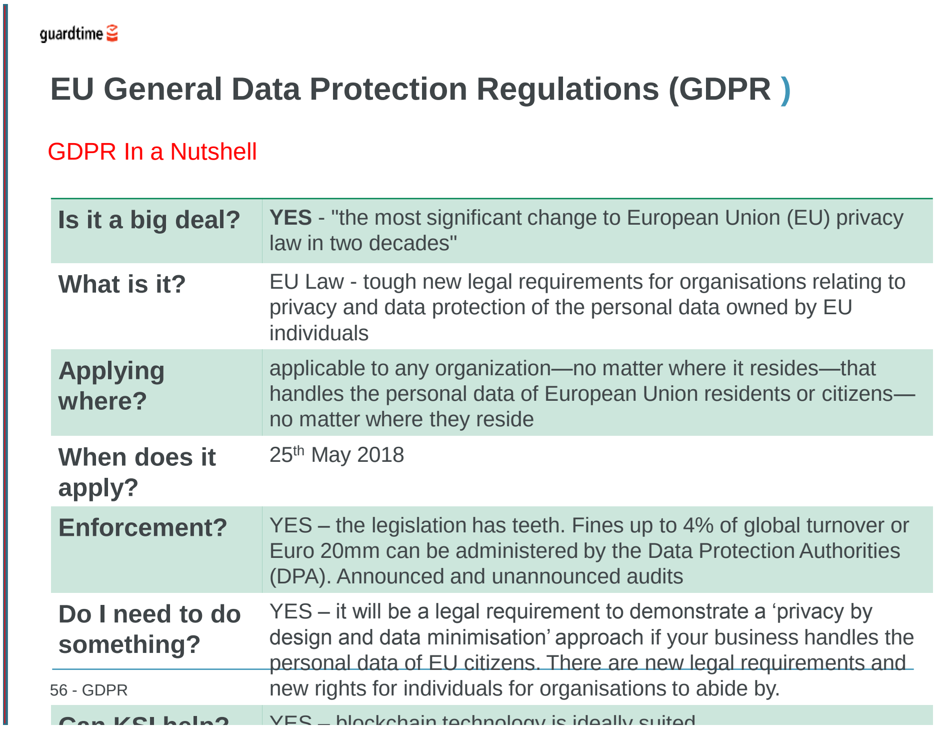
2008
SECURITY
ASSURANCE

2015
SMART
CONTRACTS

Blockchain Solutions for GDPR

DS v1.3 February 2017

guardtime



guardtime

EU General Data Protection Regulations (GDPR)

GDPR In a Nutshell

Is it a big deal?	**YES** - "the most significant change to European Union (EU) privacy law in two decades"
What is it?	EU Law - tough new legal requirements for organisations relating to privacy and data protection of the personal data owned by EU individuals
Applying where?	applicable to any organization—no matter where it resides—that handles the personal data of European Union residents or citizens—no matter where they reside
When does it apply?	25th May 2018
Enforcement?	YES – the legislation has teeth. Fines up to 4% of global turnover or Euro 20mm can be administered by the Data Protection Authorities (DPA). Announced and unannounced audits
Do I need to do something?	YES – it will be a legal requirement to demonstrate a ‘privacy by design and data minimisation’ approach if your business handles the personal data of EU citizens. There are new legal requirements and new rights for individuals for organisations to abide by.
Can KSI help?	YES – blockchain technology is ideally suited

56 - GDPR

guardtime

GDPR – New Rights of the Individual re their Personal Data

includes

Right to be Informed

Right to be informed of the personal data you hold, of how you use it, of any breach, and of any disclosure or usage to third parties

Right to Access

Right to access of own personal data, and to any processing or sharing details.

Right of Consent

Right to withdraw consent or restrict the processing or sharing of their data, including for the purposes of direct marketing.

Explicit and unambiguous consent must be obtained

Right to be Forgotten

Right to request the deletion or removal of personal data whether there is no compelling reason for its continued processing

Right to Correct

Right to rectify data if inaccurate or incomplete

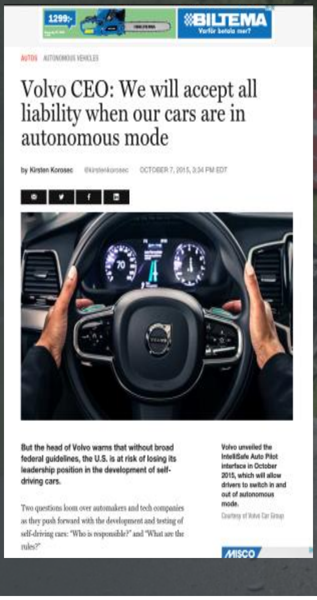
Right to Data Portability

A copy of the data held may be requested by the individual

EU comment: "**people can be sure they are in control of their personal information**"

guardtime

Who is responsible ?



AUTOS AUTONOMOUS VEHICLES

Volvo CEO: We will accept all liability when our cars are in autonomous mode

by Kirsten Korosec @kirstenkorosec OCTOBER 7, 2015, 3:34 PM EDT

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

Institute
and Faculty
of Actuaries

Key New Products

25 May 2017

guardtime

Cyber (Contingent) Business Interuption

Business & Finance

CBI

means

Contingent Business Interruption

by acronymsandslang.com

- First, Third and Fourth Party Damage – accumulation risk
- Regulatory Consequences
- Operational Technology (OT) meets Information Technology (IT)
- Increasing use of Devices and Internet of Things (IOT)
- Increased risk of critical infrastructure attacks
- Reputational Loss + (C) BI + Liability Claims Costs – economic disaster
- Because of Reputational Risk the data is not made public

guardtime

Data Compromise BI

- The silent threat – time to compromise to discovery
- Physical network can be covered as visible effects to network and partners
- As insurance based on time deduction linked to discovery mitigation is required
- Serious threat to the economic and digital supply chain
- Data must be signed by KSI in order to get notification
- All parties involved should be linked on a blockchain for maximum fraud reduction

Institute and Faculty of Actuaries

Conclusions

25 May 2017

CONCLUSIONS AND OBSERVATONS

- **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**

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 tends 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 ?.

Where is it all Going by 2018

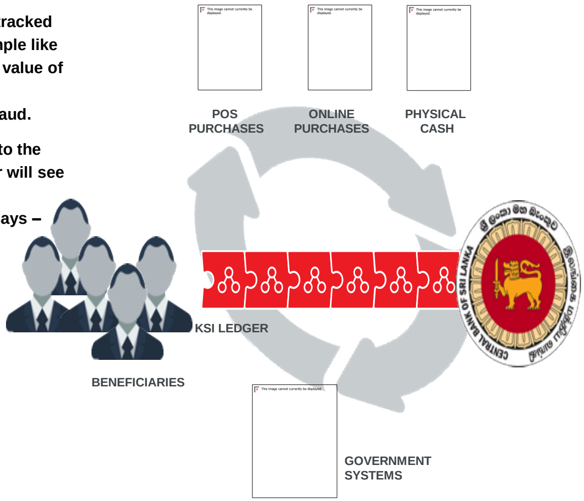
- Automation of insurance companies into a smart contract
- Automatic payment of claims – no filing claim or admin expenses
- Ability to eliminate digital fraud
- Tampered documents will be caught reducing errors and omissions
- Management by consensus for liability
- Insurance goes under the bonnet

WHERE IS BLOCKCHAIN, AI AND DIGITISATION TAKING THE INSURANCE INDUSTRY AND ALL THE BUISNESS SECTORS

National Digital Currency – the Eureka Moment for Wide Understanding

Digital Currency that can be traced, tracked and controlled. In Sri Lanka for example like other countries less of the monetary value of benefits ends up in the hands of the beneficiary – much is lost through fraud.

Once the digital currency is pegged to the national currency then the consumer will see the benefits of blockchain and data ownership. That is where everyone says – ahaaa



Blockchain value proposition spans insurance, transportation and manufacturing industries

- Liability and Subrogation Management: Addresses the fundamental question: Who is liable in the event of an accident? The blockchain provides immutable proof of what happened. With that certainty, liability can be attached and subrogation claims can be automated.
- Blockchain Based Claims Processing: Automated claims processing utilizing high fidelity data becomes possible speeding up settlement times and dramatically reducing claims fraud.
- Security Operations: Continuous monitoring of in-network firmware, software and configuration parameters triggering alerts in the event of malicious or out-of-policy updates.
- Software Supply Chain: End-to-End management of the software supply chain for firmware and software (FOTA/SOTA) in each device IOT network.
- Warranty Claims Management: The integration of KSI Blockchain enables insurers to have a complete and accurate picture of warranty validity at any point in time***.***
- An Immediate *Early Warning System* for Vehicle, System and Component Failure

Future - The Car Becomes the Moving Mobile Wallet

- **IOT includes sensor as a service by mobile payments**
- **Blockchain IOT Protocol – merge payments and IOT**
- **Pay for fuel, recharging of road tolls by smart contracts**
- **Money exchanged without banks or credit card company**
- **Eventually insurance will become invisible by blockchain**
- **Cite the INTERNET and emails**

What is the Insurance Effect in 2017

- INSURETECH Solutions will double in the market .

•InsureTech

- 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 – big data 2.0.

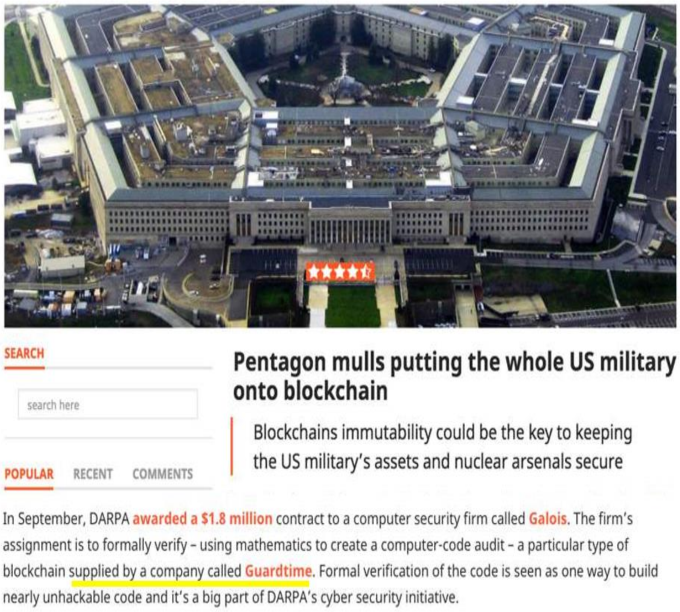
- The amount of smart devices is increasing and that will increase the need for insurance industry to understand the implications and wordings for the risk.

CoVi Analytics

- Cyber Terrorism is on the increase and governments need to work with private industry to ensure backstop.

KSI Proven in Defence

guardtime



SEARCH

search here

POPULAR RECENT COMMENTS

Pentagon mulls putting the whole US military onto blockchain

Blockchains immutability could be the key to keeping the US military's assets and nuclear arsenals secure

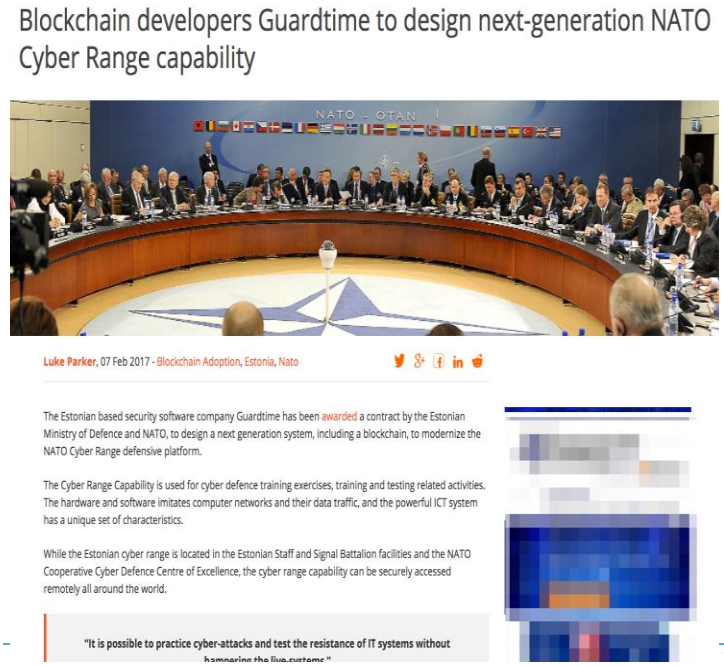
In September, DARPA awarded a $1.8 million contract to a computer security firm called Galois. The firm's assignment is to formally verify – using mathematics to create a computer-code audit – a particular type of blockchain supplied by a company called Guardtime. Formal verification of the code is seen as one way to build nearly unhackable code and it's a big part of DARPA's cyber security initiative.

guardtime

European Commission

“Guardtime Signs €450 million Strategic Alliance Agreement with EU Commission on Cyber Security”

71



Blockchain developers Guardtime to design next-generation NATO Cyber Range capability

Luke Parker, 07 Feb 2017 - Blockchain Adoption, Estonia, Nato

The Estonian based security software company Guardtime has been awarded a contract by the Estonian Ministry of Defence and NATO, to design a next generation system, including a blockchain, to modernize the NATO Cyber Range defensive platform.

The Cyber Range Capability is used for cyber defence training exercises, training and testing related activities. The hardware and software imitates computer networks and their data traffic, and the powerful ICT system has a unique set of characteristics.

While the Estonian cyber range is located in the Estonian Staff and Signal Battalion facilities and the NATO Cooperative Cyber Defence Centre of Excellence, the cyber range capability can be securely accessed remotely all around the world.

> "It is possible to practice cyber-attacks and test the resistance of IT systems without hampering the live-systems."

guardtime

Introduction

- World's Largest Blockchain Company
  - By revenue, headcount, customers
- Founded in 2007 in Tallinn, Estonia
- 150 Full-time employees

Tallinn, Estonia
Amsterdam
London
Alexandria, VA
Lausanne
Irvine, CA
Dubai

Offerings:

- Heath Care Patient Assurance
- Electronic VAT
- **Helium Insurance Platform**
- Connected Car Liability Management
- Smart Grid Assurance
- GDPR Compliance
- Digital and Physical Supply Chain

Competitive Advantage:

A battle-hardened blockchain stack, in production since 2007 with governments and enterprises relying on the platform today.

Government Deployments

Example Customers

GE
BOEING
Raytheon
EY
DARPA
NATO
LOCKHEED MARTIN
SICPA
ERICSSON

Institute and Faculty of Actuaries

Thank You Q&A

25 May 2017