# ENTERPRISE RISK MANAGEMENT

Mumbai
10 Aug 2018

## TOPIC : Information & Cyber Security Risk

Pawan Chawla
CIO & Partner

LUCIDEUS™
SECURING DIGITAL

# About Lucideus

- Incubated out of IIT Bombay, we are a pure play cyber security platforms company
- We provide IT risk assessment services and platforms to corporates and governments across the globe
- Some names in our client list include Future Generali, HSBC, Visa, ICICI Bank, SoftBank, BlackRock, Coca Cola, KFC, Indigo, Mckinsey among others
- We were responsible for the end-to-end cyber security assessment of the BHIM Payments Application recently launched by the Prime Minister of India
- We recently won the Emerging Cyber Security Vendor of the year presented by Frost and Sullivan
- In 2016 we were awarded the Best IT Startup of India by the Government of India

LUCIDEUS™
SECURING DIGITAL

# Cyber War

*You may not be interested in war, but war is interested in you*

- Leon Trotsky

LUCIDEUS™
SECURING DIGITAL

# Information Risk

**How easy is to get someone's details?**

- Watch to understand how your data can be manipulated - Link
- What a company can go through because of Social Engineering - Link

LUCIDEUS™
SECURING DIGITAL

# Cyber Security & Risk

- Cyber Security
- Cyber Risk
  - Risk Assessment
  - For an Organization
    - Cyber risk a growing nightmare?

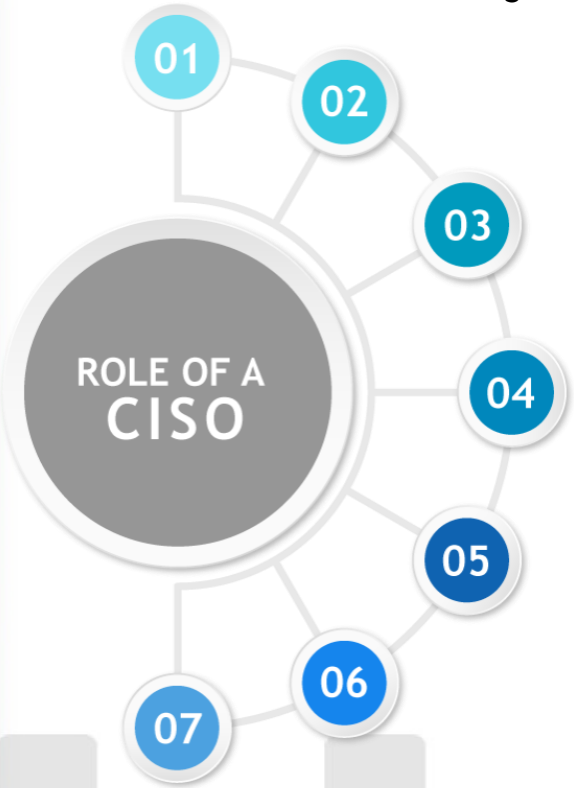
LUCIDEUS™
SECURING DIGITAL

# Cyber Risk


*“65% of companies that reported sharing customer data with a partner also reported subsequent breach through that partner ”*

LUCIDEUS™
SECURING DIGITAL

# Role of a CISO




Strategic Advisor

Chair Information Security Committee (ISC)

Represent Information Security at Board Level

Interface with Regulators and other Compliance Regimes

Information Security Architecture and Design

Deliver Information Security Projects

Manage Security Services

LUCIDEUS™
SECURING DIGITAL

# Current Cyber Risk Underwriting Scenario

Underwriting for cybersecurity is currently based on either of the following:

- **External Cybersecurity Score** which
  - is not considering the **security requirements** of the company
  - is not factoring in the **internal changes** within the company and
  - is based on **incomplete information**

- **Questionnaire Based Assessment** which
  - Suffers from **information asymmetry** due to differing outlooks towards a company's cybersecurity postures
  - Compromises the **completeness of information** to save time

LUCIDEUS™
SECURING DIGITAL

# Why is Cyber Risk Transfer Important?

Likelihood is not low enough to ignore & the impact is to massive to handle

Cyber Risk is not included in current **ERMs**

**Shareholders and Customers** are being kept in the dark

**Balance Sheets and Market Caps** are not Protected

LUCIDEUS™
SECURING DIGITAL

# Challenges in **Cyber Risk Transfer**

- **Damage Valuation** is highly unpredictable before and after the breach
- **Unwillingness to report breaches** in fears of escalations
- **Threat and Breach data** is unavailable and non-standardized
- Inability to accurately estimate the **likelihood of breach**

LUCIDEUS™
SECURING DIGITAL

# Case Studies

**Target Corporation** experienced a data breach in 2013, which exposed the personal information of more than 100 million customers

- **Impact of Breach -** $291 million
- **Covered by Insurance -** $100 million with $10 million deductible
- **Bad Decisions -** Improper Business Impact Analysis prior to insurance offering

After sonypictures.com was breached in 2011, which resulted in 37,000 people having PII exposed, **Sony Pictures** made a claim of $1.6 million with Hiscox, their cyber insurance carrier at the time

- **Impact of Breach -** $15 million
- **Covered by Insurance -** Nil
- **Bad Decisions -** Improper Policy Coverage

LUCIDEUS™
SECURING DIGITAL

# Case Studies

In June 2014, hackers obtained and posted on the internet approximately 60,000 credit card numbers belonging to **P.F. Chang's** customers.

- **Impact of Attack -** $3.6 million
- **Covered by Insurance -** $1.7 million
- **Bad Decisions -** Certain exclusions in the insurance policy that barred coverage for MasterCard's fees and assessments

Hackers used phishing emails to break into a **Virginia bank** in two separate cyber intrusions. The bank had 2 types of coverage - "computer and electronic crime" that had a single loss limit liability of $8 million and "debit card" which had a single loss limit liability of $50,000

- **Impact of Attack -** $2.4 million
- **Covered by Insurance -** $50,000 for both intrusions
- **Bad Decisions -** Exclusions in the insurance policy that gave limited coverage for debit card breaches

LUCIDEUS™
SECURING DIGITAL

# Key desirable attributes proposed by *World Economic Forum for Cyber Risk Model*

- **Applicability:** Ability to apply the model across different industries and adjust it depending on the needs of the company
- **Precision:** Comprehensiveness and measurement accuracy and precision of the model
- **Timeliness:** Ability to timely reflect the environment around the incidents
- **Scope:** Ability to cover a wide range of factors and risks
- **Decision-making process:** Potential to serve as an effective risk measurement tool for executives and decision-makers

*Reference: *WEF (in collaboration with Deloitte); Partnering for Cyber Resilience Towards the Quantification of Cyber Threats(2015)*

LUCIDEUS™
SECURING DIGITAL

# Cyber Risk Measurement for Security of Enterprises

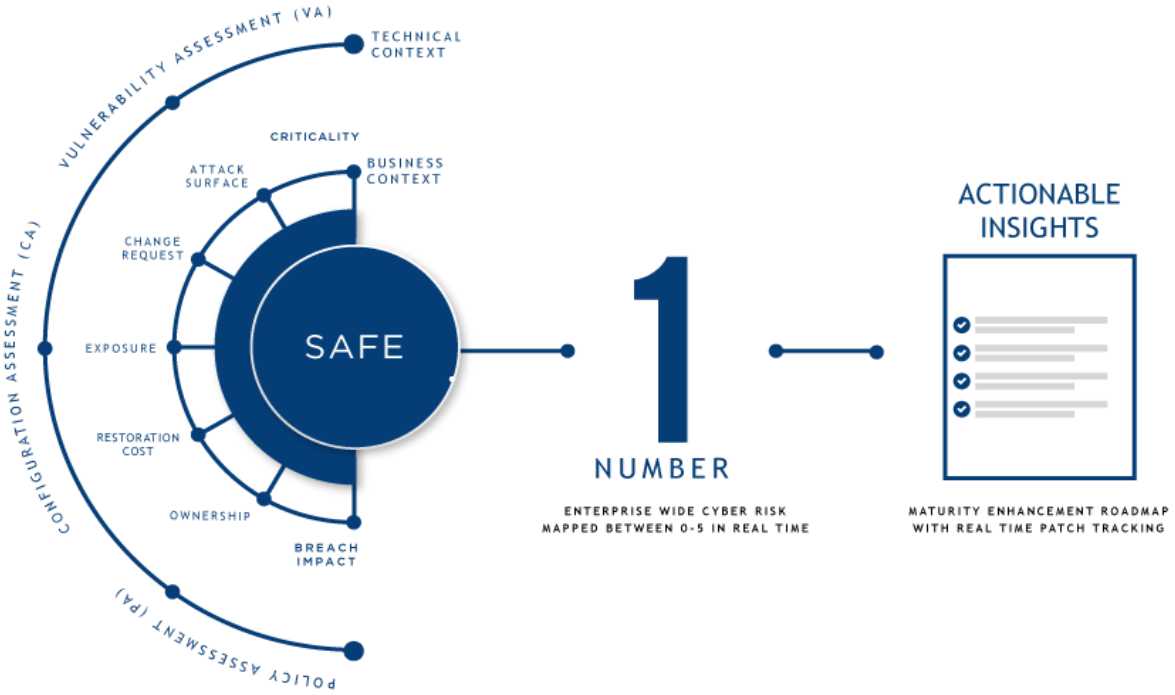

#SAFEScore

*The Average Cost Of A Data Breach was $3.62 Million In 2017**

**SOURCE: IBM SECURITY REPORT 2017*

LUCIDEUS™
SECURING DIGITAL

# How SAFE works




LUCIDEUS™
SECURING DIGITAL

# Technology Stack Buildup


- On premise cloud synced deployment
- SaaS based cloud service model
- Enterprise mobility modules
  - iOS
  - Android
- Proprietary & patent pending algorithm
- 1.2 million lines of code
- 2500+ controls for over 12 verticals

MOBILE APP | WEB APP | THICK CLIENT APP | SERVERS

CLOUD | NETWORK NODES | ENDPOINT | MOBILE DEVICE

IOT DEVICES | STORAGE | SCADA | DATABASE

LUCIDEUS™
SECURING DIGITAL

# Properties / Attributes of SAFE Score

**Real-Time**

Automated assessments gives near real time scoring for dynamic factors

**Up To Date coverage of threat landscape**

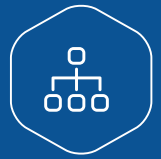
Updated with latest threat feeds and control libraries from global industry standards

**Risk Quantification**

It quantifies and helps in measuring the cyber security risk posture of an organization

**Cognitive Security**

Backed by AI / ML



**100% Tech stack coverage**

Covers 100% assets
Covers Internal & External risk

**Prelude to Insurance**

It monitors the risk across the policy period

# SAFE Score to drive Cyber Risk Transfer

- Better **Breach Likelihood** predictions
- **Moral Hazard** addressed with Real Time Assessment
- Control Claims from **Pandemic Breaches** with fast feedback engine
- **Adverse Selection** answered by Complete Information
- Coverage of a **Long List of Breaches** and Adverse Events
- **Model that Learns and Improves** with every claim data
- **Monitors Efforts and Outputs** in Cyber Security

LUCIDEUS™
SECURING DIGITAL

# Adverse impact of a Breach

An **Adverse Event** is an event that an adversary can create against a company resulting in a **loss to the Company**.

1. Productivity Loss
2. Reputation Loss
3. Competitive Advantage Loss
4. Response Cost
5. Replacement Cost
6. Fines & Jurisdiction Cost

Damage factors that require Insurance Cover

LUCIDEUS™
SECURING DIGITAL

# Challenges related to **Adverse Events**

- Likelihood of an adverse event is too volatile and too uncertain for prediction
- Damage value is unpredictable for calculating limit of liability as well as claims

LUCIDEUS™
SECURING DIGITAL

# Risk Assessment enabled by SAFE and Lucideus

LUCIDEUS™
SECURING DIGITAL

# Cyber Risk Assessment

## 1 First Contact

**Insurer and Insured** explore the possible scenarios and get Initial Information

## 2 Processing Initial Information

**Lucideus** process the information provided to it and prepare for next steps

## 3 Triad Meeting to determine the Scope of insurance

**Lucideus** meets Insurer and Insured to get a list of possible Incidents that need Insurance Policy

## 4 Business Impact Analysis

Business Impact Analysis is done to get **minimum, maximum, and mode** of the impact of different incidents in various loss factors

## 5 Prediction for Likelihood of the Incidents

**Lucideus** provides the prediction of likelihood of the individual Incidents if the company maintains one of the given SAFE standards

LUCIDEUS™
SECURING DIGITAL

# Policy Selection & SAFE Installation

## 6 First Offerings

Based on the business impact and the likelihood values a **number of policies** are formulated and offered to the insured.

## 7 Selection of Policy

**Insured** is required to **choose one policy** as per the business risk preference

## 8 Installation of SAFE

**SAFE** is installed at Insured's premises and then **customized to include groups of assets** that enables different incidents covered under chosen policy.

## 9 Insurance Dashboard

Insurer's dashboard of **SAFE** gets an update with the features relevant to the policy including the SAFE score of the Groups created above.

LUCIDEUS™
SECURING DIGITAL

# Process for Claims

## 10 Breach

Policy enforces the insured to **provide details of the breach through SAFE** for every breach.

## 11 Forensics

Incidence response, Root cause analysis and Fraud Investigation is performed by **Lucideus**

## 12 Business Impact Analysis

**Estimation of business loss/cost** associated with the breach is performed

## 13 Claim

The claim amount will be calculated as per the **results of forensics & business impact analysis**

LUCIDEUS™
SECURING DIGITAL

# Response by SAFE

## 14 Forensics & Business Impact Reports

SAFE absorbs the **Forensics & Business Impact reports** associated with the breach as they are generated

## 15 Identification of Critical Breach Factors

SAFE will identify the c**ritical factors that caused** the breach and update the respective control lists

## 16 Re-assessment of defence for other SAFE instances

**SAFE** score is re-computed with the updated control list

## 17 Increase defence

**SAFE will generate a task list** factoring in the impact of updated control list and the policy will enforce the organization to finish the task within a specified time

LUCIDEUS™
SECURING DIGITAL

# Uncertainty in the likelihood of **Adverse Events**

Prediction of the likelihood of an adverse event is the key challenge in cyber security underwriting

$$\pi(\mathcal{A}) \quad \text{vs} \quad \pi(\mathcal{A}|\mathcal{S})$$

Answer uncertainty through **SAFE Score**

LUCIDEUS™
SECURING DIGITAL

# Likelihood of an Adverse Event through SAFE Score

Bayes' Theorem yields

$$\pi\left(\mathcal{A}|\mathcal{S}\right) = \pi\left(\mathcal{A}\right) \times \frac{\pi(\mathcal{S}|\mathcal{A})}{\pi(\mathcal{S})}$$

Where **A** is the event that an adverse event happens to a company with given data within a year and **S** is the event that the SAFE score lies in a given range.

LUCIDEUS™
SECURING DIGITAL

# Prediction of the Likelihood of **Adverse Event**

$$\pi(\mathcal{A}) \quad \text{vs} \quad \pi(\mathcal{A}|\mathcal{S})$$

with or without complete cyber resilience information

Likelihood of an adverse event with no consideration to the security status of a company is just too **volatile and uncertain.**

SAFE scores depends on complete **cybersecurity information** about a company's cyber defense

Prediction of likelihood of an adverse event becomes highly accurate with SAFE Score

LUCIDEUS™
SECURING DIGITAL

# SAFE Score Standard for **Cyber Risk Transfer**

$$\frac{\pi(\mathcal{S}|\mathcal{A})}{\pi(\mathcal{S})}$$

Breach likelihood for companies, with high SAFE score, drops down drastically providing ideal conditions for cyber risk transfer

SAFE score is designed to be proportional to the cyber defense of a company. Hence, for the upper range of SAFE score the above factor is going to be extremely low.

LUCIDEUS™
SECURING DIGITAL

# Objective

## Maximize utility/satisfaction level by optimizing budget

## Expected Utility

= Expected Utility at No Loss State + Expected Utility at Loss State

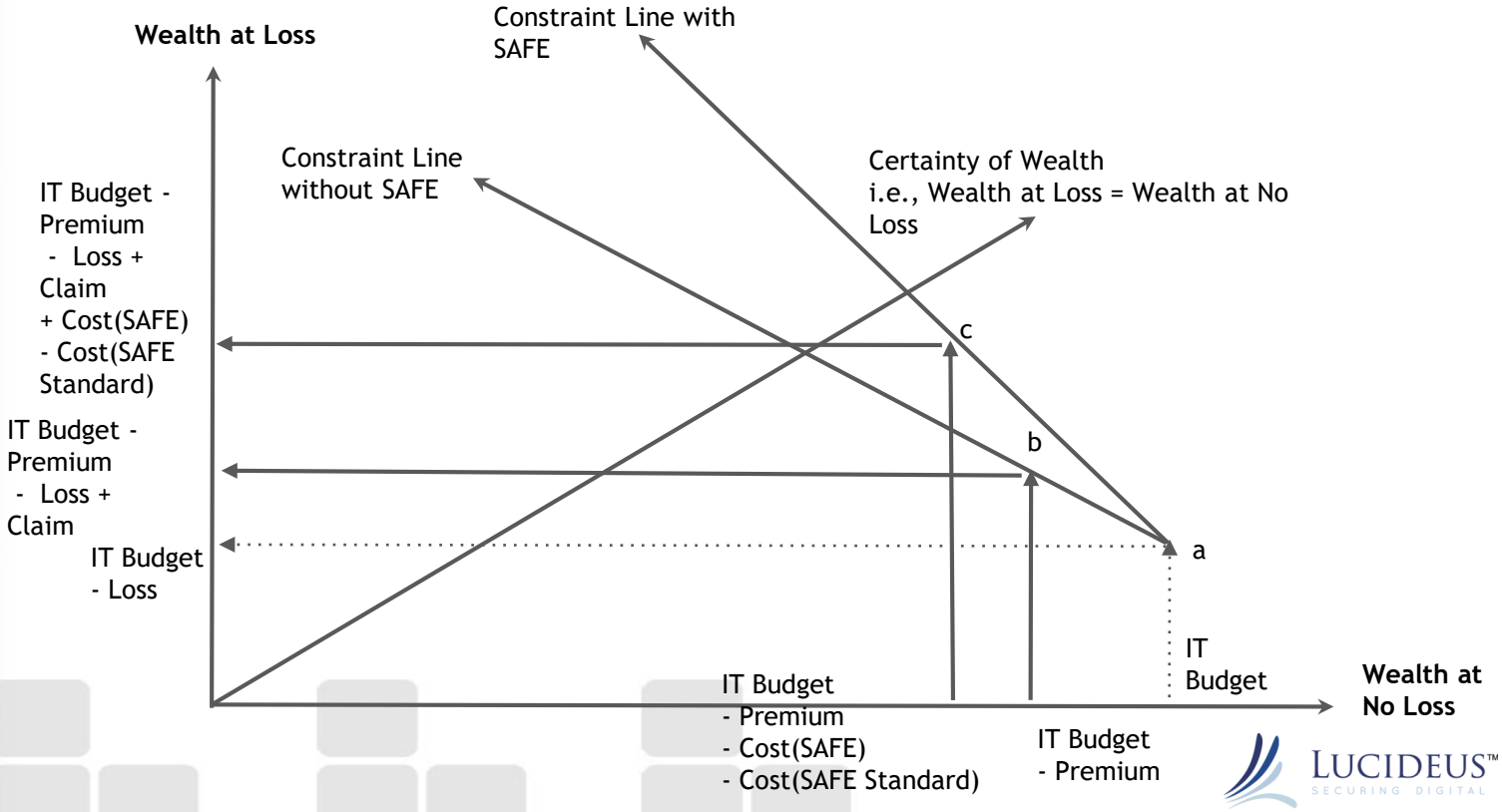
= [ Likelihood of No Loss × Utility at No Loss ] + [ Likelihood of Loss × Utility at Loss ]

= $(1 - \pi(\mathcal{A}|\mathcal{S}))$ × Utility at No Loss given IT Budget - Premium - Cost of SAFE Subscription - Cost of Maintaining SAFE Standard

+ $\pi(\mathcal{A}|\mathcal{S})$ × Utility at Loss given IT Budget - Premium - Cost of SAFE Subscription - Cost of Maintaining SAFE Standard - Loss + Cover from Claim

LUCIDEUS™
SECURING DIGITAL

# Budget Constraint Graph




LUCIDEUS™
SECURING DIGITAL

# Objective of an Organization

## Risk Pooling

It is the result of insuring lots of individual people or businesses and expecting that most losses will result in only having to pay claims to some of the insured.

## Risk Spreading

The risk is spread among many insurers or syndicates so that each holder has a sufficiently small stake in any possible outcome.

## Maximize

Profit = Earned Premium + Investment Income – Claim – Underwriting Expenses

# Adverse Selection addressed by SAFE

**Problem**: Insurer's Lack of visibility about insured's risk type

- Insured has better **visibility about their risk type** than the insurer and are **resistant to share complete information** with the insurer.

**Solution**: SAFE Score

- SAFE score **reduces the asymmetric information about the insured risk** by producing a score for the insured. Also, it helps to understand the probability ($\pi$) of the risk involved.

LUCIDEUS™
SECURING DIGITAL

# Moral hazard addressed by SAFE

**Problem** : Moral Hazard in IT industry

- Most companies in the IT industry tend to show **little incentive to prevent any cyber attack,** and on top of that if they get insurance with full cover against any loss due to this phenomena their incentive will only decrease

**Solution**: SAFE Score

- SAFE score is a **real-time measure** of the cybersecurity. This property **helps insurer to monitor the effort** of any firm in maintaining a specific SAFE score throughout the insurance/policy period. Thereby, preventing itself from any loss due to the moral hazard problem.

LUCIDEUS™
SECURING DIGITAL

# Improving accuracy of SAFE Model using **Machine Learning**

SAFE has the ability of self improvement with observations.

SAFE is built on a machine learning principal where it is able to improve itself with the help of a collection of breach data so as to be able to reflect the breaches more appropriately in the later versions.

Thus, the claim data can be re-utilized in SAFE which will further **enhance its capability of handling Pandemic Breach situations.**

LUCIDEUS™
SECURING DIGITAL


LUCIDEUS™
SECURING DIGITAL