

SAS ERM - ESSEC CREAR Conference 2018



SINGAPORE
ACTUARIAL
SOCIETY



HACKING ALERT



Cyber risks – Threats and Opportunities for the Asia Pacific Insurance Industry





Insurance Cyber Risks – Regulations and Development - Mitigating solution

Srinivas Bhoosarapu

Lead Auditor -ISMS ISO 27001

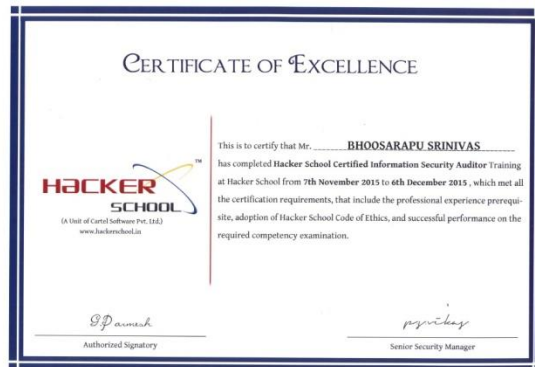
IRDAI, Hyderabad





Indian Cyber Security Initiatives – Case Study

Srinivas Bhoosarapu
Lead Auditor -ISMS ISO 27001



INDIAN INSTITUTE OF QUALITY MANAGEMENT

CERTIFICATE

of

Attendance

This is to certify that

Srinivas Bhoosarapu

has Successfully Completed the

INFORMATION SECURITY MANAGEMENT SYSTEMS (ISMS)

AUDITOR/ LEAD AUDITOR TRAINING COURSE

Course No. : A 17226 Certified by IRCA

Course Venue : **STQC IT Services, Hyderabad**

Date of Course : **16th to 20th December 2013**

Certificate No : **IIQM/TRG/R/187/2014**

M. S. Bhoosarapu
Course Coordinator
Date : 14.03.2014

M. S. Bhoosarapu
Director



STQC Directorate, Govt. of India, Dept. of Electronics and IT,
Ministry of Communications and Information Technology
Malviya Industrial Area, Jaipur, India, 302017



Learning outcome Agenda

Å **Cyber Risk – Insurance**

Å **Core Insurance System & Data Breaches in Insurance System**

Å **Threats Landscape – Challenges - Opportunities**

Å **Regulations and Development**

Å **Counter Measure , Mitigating Solutions and Controls**

Å **Indian Cyber Security Initiatives - Use Cases**

Cyber Risk – Insurance Sector

Å Cyber Risk - “The combination of the probability of an event occurring within the realm of an organisation’s information assets, computer and communication resources and the consequences of that event for an organisation.”

Å Insurance Sector - Identified several additional cyber security incidents experienced by insurers in multiple jurisdictions, including attacks against personal lines, travel, health, and marine insurers.

Cyber Risk – Insurance Sector

As Cyber risk presents a growing challenge for the insurance sector, to address. Insurers collect, store, and manage substantial volumes of confidential personal and commercial information.

At these reservoirs of data, insurers are prime targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other criminal activities.

In addition, because insurers are significant contributors to the global financial sector, interruptions of insurers' systems due to cyber security incidents may have far-reaching implications.

Cyber Risk - Insurance

High Profile Data Breaches, 2013-2014



Date	Company	Description of Breach
May 2014	EBay	Massive data breach exposed records of site's 233 million customers, including names, email addresses, physical addresses, phone numbers and birthdates.
Feb 2014	Michaels Stores	Possible fraudulent activity on some U.S. payment cards used at Michaels stores suggests it may have experienced data security attack, exposing 2.6 million records.
Jan 2014	Neiman Marcus	Hacker break-in exposed unknown number of customer cards, compromising estimated 1.1 million records.
Dec 2013	JPMorgan Chase	Hackers attacked banking giant's network, compromising some personal information of 465,000 card holders.
Nov/Dec 2013	Target	Malware stored on Target's checkout registers led to theft of data from about 40 million credit and debit card accounts and the personal information of up to 70 million customers.
October 2013	CA-based AHMC Hospitals	Two unencrypted laptops stolen compromising patient information, including names, social security numbers, and diagnostic codes, jeopardizing 729,000 patients.
Aug/Sept 2013	Adobe	Hackers stole encrypted customer credit card information and other data for 38 million users.
July 2013	Dept of Energy	Leak of over 104,000 employees' and contractors' personal information, including name, social security number, date of birth. Attack leveraged flaw in Adobe product.
April 2013	Living Social	Hackers stole personal data, including names, emails, birthdates and encrypted passwords of more than 50 million users.
Jan 2013	New York Times	Chinese hackers infiltrated New York Times computer systems for a period of four months, getting passwords for its reporters and employees.
Dec 2012	Google, Facebook, LinkedIn, Twitter, Yahoo and ADP	Cybercriminals stole 2 million passwords and user names with a botnet known as 'Pony' from Google, Facebook, Twitter and Yahoo. Nearly 100 countries hit.

Sources: Identity Theft Resource Center; Insurance Information Institute (I.I.I.) research.

Incidents

Cybersecurity Incidents in the Insurance Sector

The insurance sector has experienced a variety of cybersecurity incidents in recent years, including well-publicised data breaches at several U.S. health insurers. Some examples of these cybersecurity incidents are provided below.

In 2015, Anthem Blue Cross Blue Shield and Premera Blue Cross experienced data breaches in which credit card data and personally identifiable information, including health data, were compromised.²³ The breaches potentially exposed the personal information of up to 91 million policyholders – as many as a quarter of the people in the United States.²⁴ The insurers had to react swiftly to mitigate reputational damage and to minimise litigation costs, although it is currently unknown how much loss the insurers will ultimately incur due to this breach.

In another recent U.S. example, a data server operated by the state of North Dakota was compromised, potentially exposing a range of personal information related to workers compensation claimants – including 43,000 Incident Reports and 13,000 Payroll Reports that had been filed online by workers and employers. Reportedly, medical information and claim files were not exposed, but data at risk was said to include individuals' names, social security numbers, birth dates, descriptions of injury, descriptions of incidents, names of employers, and employer addresses.²⁵

A group of cyber extortionists known as the “DD4BC” has been targeting a range of firms including financial institutions in Europe, Australia, Canada, and the United States with threats of distributed denial-of-service (DDoS)²⁶ attacks in order to extort money from them. DD4BC has demanded ransoms of varying amounts, to be paid in bitcoins (crypto-currency), threatening to launch DDoS attacks unless the target pays the ransom by a specified deadline. Two German insurance groups experienced this type of attack in mid-2015, receiving threats of a DDoS-attack on company web servers unless they paid 40 bitcoins. The insurers refused, as they assessed the extortionists would have caused only minor damage in those instances, but these incidents could have been far more serious if the attacks had concentrated on more critical systems.

In 2015, penetration testing performed by the internal audit team of an insurer in France found that unauthorised access to accounting tools had occurred. Although in this instance there were no further consequences, this cybersecurity incident could have had a substantial impact not only on the company but also on partners, service providers, and policyholders.

Cost of Data Breach

The Cost of Data Breach

Data breach hits organizations squarely in the wallet. The average cost per record goes up depending on who or what caused the exposure.



Source: Ponemon Institute 2015, Cost of Data Breach Study: Global Analysis



Code42 is a SaaS provider of enterprise endpoint data protection and security. We offer highly secure cloud backup to support recovery from data loss, compliance with data privacy regulations, and higher order data tools including eDiscovery and data movement analytics. www.code42.com.

Cyber Risk - Posture



Data - Breach



Global and country-specific averages show that the cost of a data breach is on the rise.

Cost per record*

Global average

\$154

12%

increase over two years

Highest countries



\$217
in the U.S.

\$211
in Germany

\$78
in Brazil

\$56
in India



Lowest countries

Cost per incident*

Global average

\$3.8M

23%

increase over two years

Highest countries



\$6.5M
in the U.S.

\$4.9M
in Germany

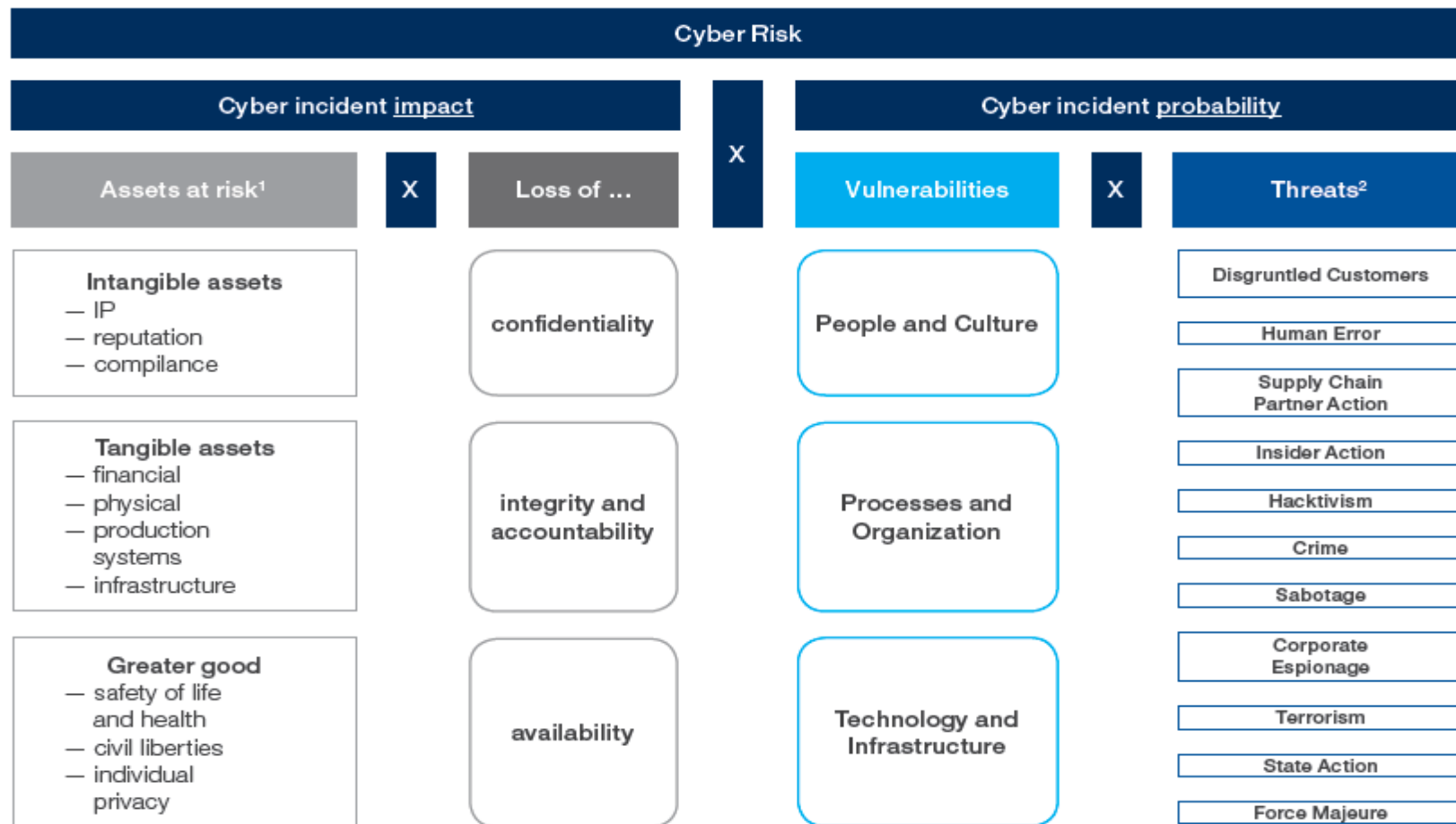
\$1.8M
in Brazil

\$1.5M
in India



Lowest countries

CIA



¹ Examples for assets

² Selection of examples, sorted in ascending order of available resources

Insurance System

- Å In general, the insurance sector faces cyber risk;
- Å From both internal and external sources
- Å Third parties.
- Å Insurers collect, process, and store substantial volumes of data
- Å Personally identifiable information. (PII)

Insurance System

Insurers are connected to other financial institutions

Å **Multiple channels**

Å **Investment**

Å **Capital raising**

Å **Debt issuance activities**

Å **Insurers outsource a variety of services.**

Å **Exposure to cyber risk.**

Effects of Cyber Threats

Å Severe and lingering harm for the policyholders

Å Significant legal.

Å Regulatory.

Å Operational costs.

Å Reputational damage.

Å Loss in public trust.

Emerging trend in Threats

Å **Critical Infrastructure – Smart Cities, SCADA, Power Grids, DCs, Transportation , Metro Rails**

Å **Critical Services - Financial Systems , Health care , Aviation, Tele Communication**

Å **Next Generation Solutions - IoT Solutions , Block Chain, SMAC**

Å **eGovernance Solutions**

Å **Human Behavioral - Cyber Terrorism**

Critical Infrastructure

Critical Infrastructures in Telangana

Transport

Road Length – **89, 758** km
Vehicle Population – **6.83** million
Railway Stations – **86**
Airport – **01**



Communication & Postal

Telephone Connections – **7.98** lakh
Telephone Exchanges – **1, 771**
Post offices – **857**



Bank

Commercial Bank
Branches – **4, 792**
ATMs – **9, 801**



Power

Major Power Plants – **24**
Distribution Transformers – **4.84** lakhs
Transmission Lines – **16, 454** CKM
Sub- Stations – **2, 341**
Transmission loss – **3.38%**



Education

Universities – **20**
Professional Colleges – **957**
General Colleges – **2, 977**
Schools – **45, 735**
Total Enrolment – **6.08** million



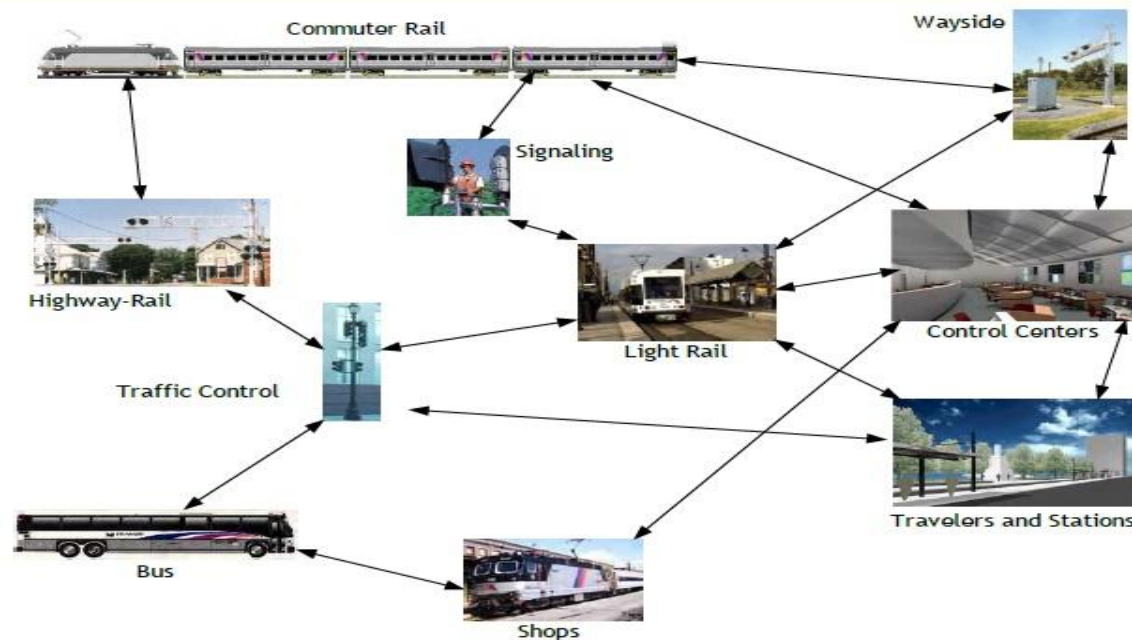
Industry

Major Govt. & Private
Companies – **42, 390**
Notified SEZ – **45**



Rail Systems

Rail Transit Communication Links



IT and Cyber Security in Metro Rail Transit System

Rail Systems - Security

A transit agency has to combine dozens of systems, including the following:

- access control systems
- advertising
- closed-circuit television (CCTV)
- control and communication
- credit card processing
- detection systems for environmental threats (CO, CO₂, poisons)
- emergency communications
- emergency notification
- emergency ventilation systems
- fare sales/collection
- fire detection/alarms/fire suppression
- grade crossings
- lighting
- passenger information systems
- people-moving systems (elevators, escalators, people movers)
- police dispatch
- pumping systems
- signals and train control
- ticketing systems
- traction power
- vertical lift devices (elevators, escalators)
- vital communication-based train control (CBTC), automatic train protection (ATP) and signaling

Next Gen Technologies

The world is changing

Big Data



90%

of the data created in the last two years alone.

Mobile



1 billion (plus)

(plus) smart devices shipped in 2013 alone.

Social



81%

of customers depend on social sites for purchasing advice.

Cloud



62%

of total workloads will be in the cloud by 2016.

Internet of Things



50 billion

devices connected to the internet by 2020.

API Economy



Global m-commerce sales were

85 billion

in 2013 and forecast to rise to \$120 billion by 2015 and an estimated \$1 trillion by 2017

Challenges

- Å **Assessment of Loss Due to Cyber Attack**
- Å **Claim Analysis in disruption**
- Å **New Product Development for Cyber Insurance for Cyber Crimes**

Opportunities to reduce the risk

Å **Vulnerability & Threat Assessment**

Å **Cyber Liability Insurance Products for emerging Solutions**

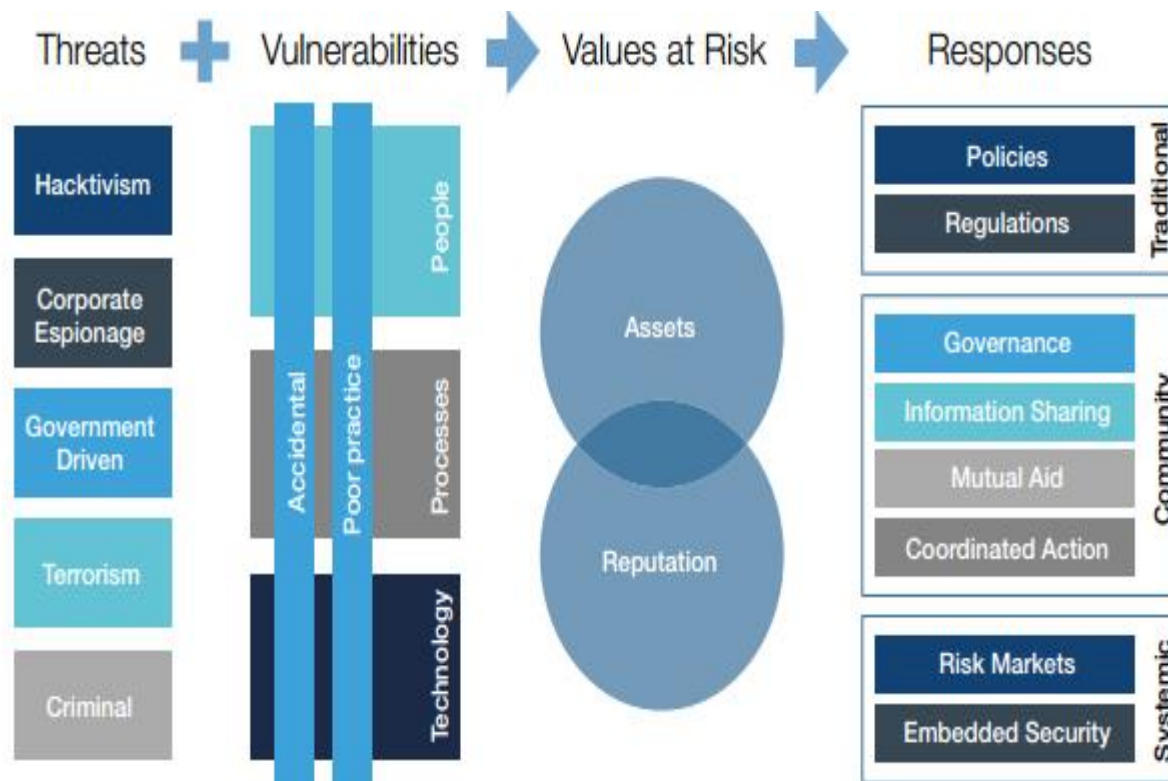
Å **Skill Development in Cyber Security Monitoring**
Security Operation Center
Network Operation Center

Å **Countering cyber risk**

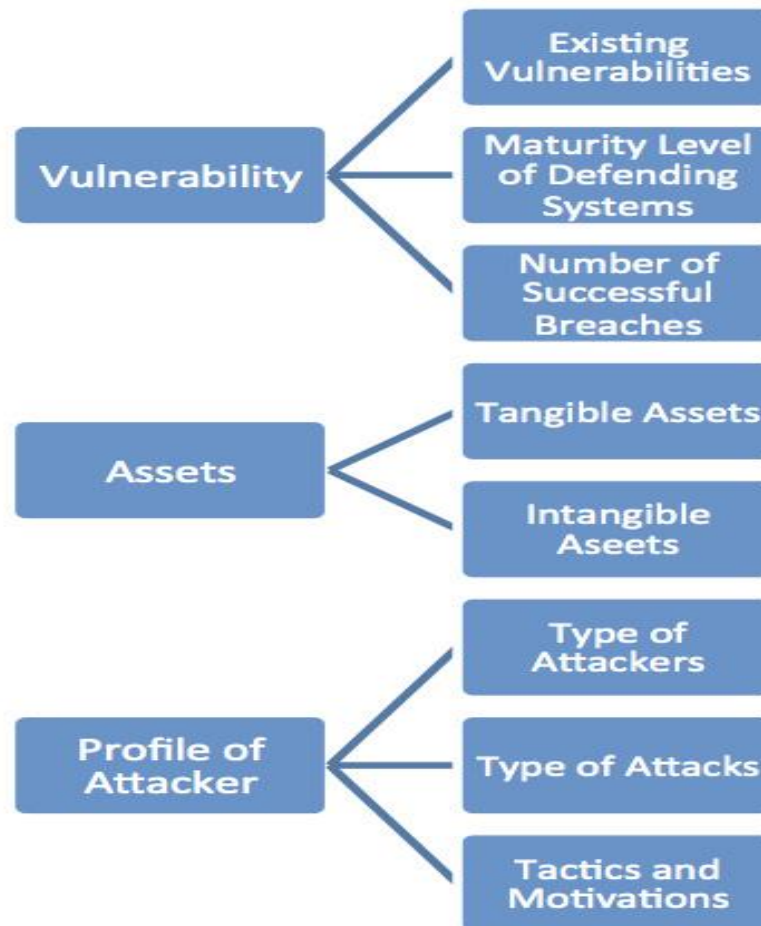
Å **Security Auditing Assessment Skill & Standards (ISO 27000 series, COBIT, TOGAF, CISA)**

Å **Awareness on Cyber Security (People , Process and Technology)**

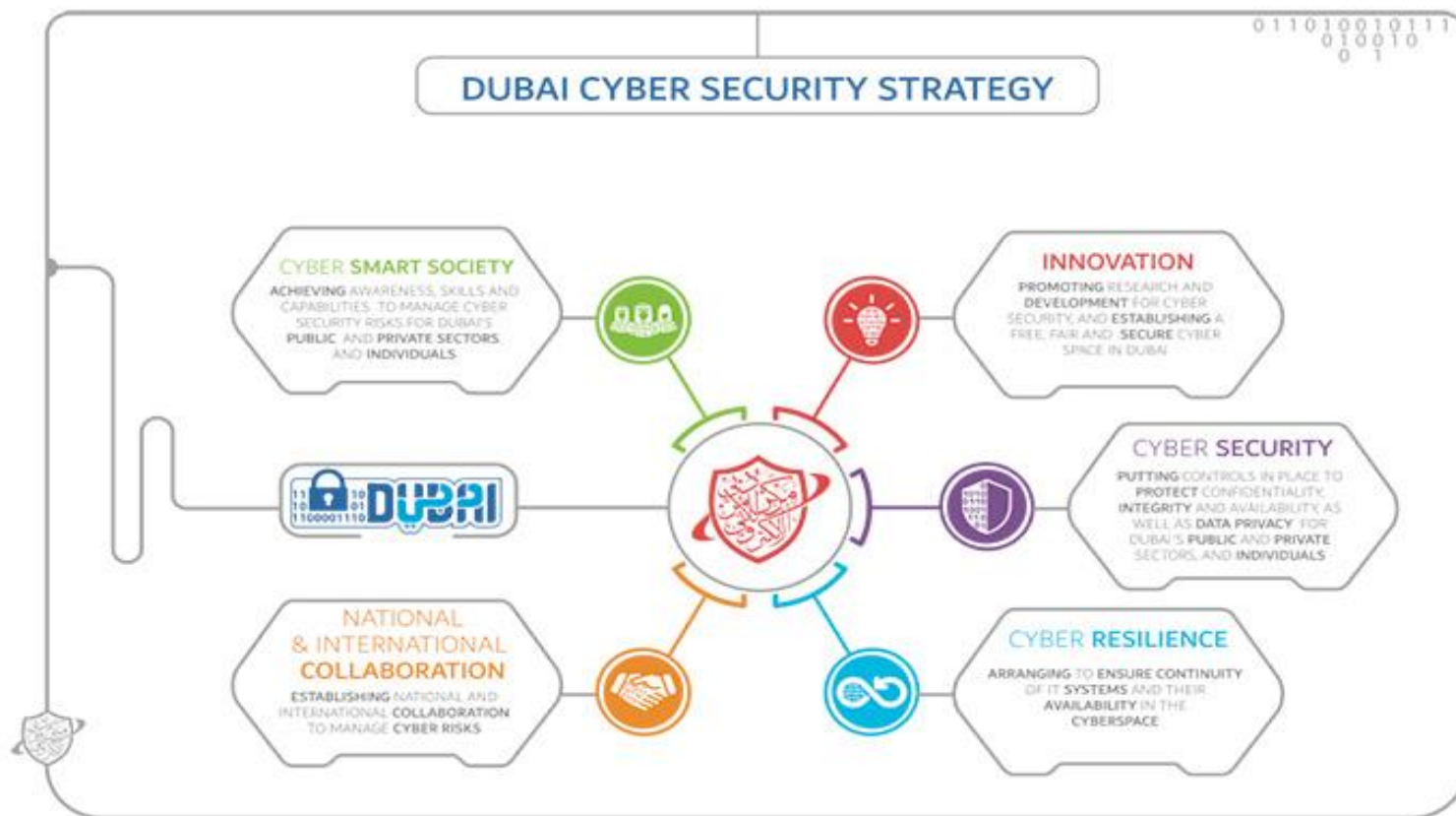
Parameter for Assessment - Challenge



Cyber Liability Product Development



Developing Cyber Security Strategy



Information Security – IT Security

Main differences between Information Security and IT Security

INFORMATION SECURITY

Strategic Area:

- Security Framework
- Policy Development
- Awareness campaigns
- Security Procedures
- Business Continuity
 - ISMS
 - Risk Analysis
 - Best Practices
 - Data Privacy
- Crisis Management
- IS Director Plan
- Organizational View
- Security Regardless of Tech
- Regulatory Compliance
- Establish Governance Model
- Etc...

≠

IT SECURITY

Technical Area:

- Hardware Hardening
- Incident Response
 - Firewalls
 - Antivirus
 - IDS/IPS
- Vulnerability Scans
- Penetration Testing
- Data Loss Prevention Tool
- Computer Forensics
 - Access Control
 - System Security
 - Network Security
- System Monitoring
- IT Disaster Recovery
 - Code Analysis
 - Etc...

Regulations and Development

Insurance Core Principles (ICPs) do not specifically address cyber risk and cyber resilience, they provide a general basis for supervisors to address the insurance sector with respect to cyber risk and cyber resilience by requiring the management of significant risks and related internal controls.

Å ICP 7 (Corporate Governance)

Å ICP 8 (Risk Management and Internal Controls)

Å ICP 9 (Supervisory Review and Reporting)

Å ICP 19 (Conduct of Business)

Å ICP 21 (Countering Fraud in Insurance)

Regulations and Development

Particularly regarding information exchange and supervisory cooperation, the following ICPs are relevant as well:

ÅICP 3 (Information Exchange and Confidentiality Requirements)

ÅICP 25 (Supervisory Cooperation and Coordination)

ÅICP 26 (Cross-border Cooperation and Coordination on Crisis Management).

Counter Measures Controls

- Å Counter Measures
- Å Mitigating Solutions
- Å Controls

Security breach: SBI blocks over 6L debit cards

Many Banks' ATMs Hit By Malware, Says Top Official

Satyanarayan Iyer
@timesgroup.com

Pune: In one of the biggest card replacements in Indian banking, State Bank of India has said that it will re-issue around six lakh debit cards to customers, which have been blocked following a malware-related security breach in a non-SBI ATM network.

"It's a security breach, but not in our banks' systems. Many other banks also have this breach, right now and since a long time," Shiv Kumar Bhasin, SBI's chief technology officer told TOI, adding that customers who used their cards only at SBI-run ATMs have not been affected by this.

"A few ATMs have been affected by a malware. When people use their card on infected switches or ATMs, there is a high probability that their data will be compromised," Bhasin said.

Several customers of the bank have found their ATM cards to be blocked. SBI has informed branches about the cards being blocked and fresh cards would be issued to customers. "Customers need not panic. They can either approach their branch, call up phone banking or use the internet for re-carding. They can also set their PINs from their homes using internet banking," Bhasin said.

Last month, Yes Bank had confirmed that its ATM network manager Hitachi Payments was re-

viewing its network to rule out any compromise. Hitachi had initiated a detailed audit of their systems through a certified agency SISA. "The preliminary reports of the audit conducted have been submitted... and the report does not establish any system-level breach at Hitachi Payment Services," the bank said.

At present, the RBI does not require banks to report to the public any security breach in their net-

BIGGER WORRY

- > ATMs of other banks affected by malware, an SBI official said
- > The malware can collect sensitive information, which can be used for financial fraud
- > Banks have to come forward and weed out compromised ATMs — something they have not done yet

work. "Banks whose ATMs have been infected must come forward and declare those infected ATMs. The onus is on them to stop this," Bhasin said, without naming the banks. He added that until the problem is addressed customers who use their cards in the ATMs of affected banks will continue to be at risk.

A branch manager in Pune confirmed that the bank has blocked a few of its customers' cards. She also said that the bank has sent SMSes to customers informing them that their card was blocked. However, affected customers were largely clueless about this development.

Most used Password

The top 50 most commonly used passwords

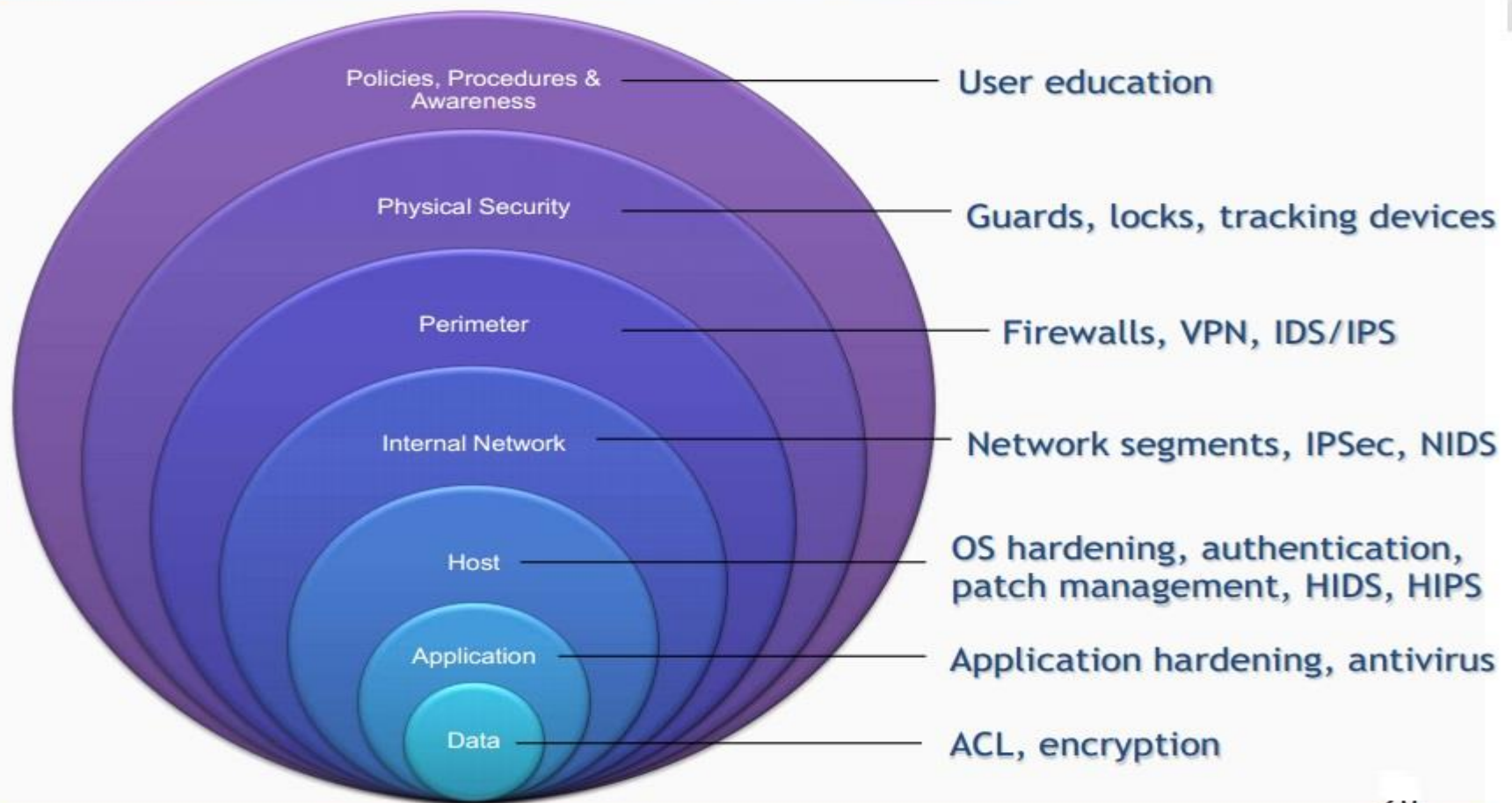
- | | | | | |
|--------------|--------------|----------------|--------------|-------------|
| 1. 123456 | 11. 123123 | 21. mustang | 31. 7777777 | 41. harley |
| 2. password | 12. baseball | 22. 666666 | 32. f*cky*u | 42. zxcvbnm |
| 3. 12345678 | 13. abc123 | 23. qwertyuiop | 33. qazwsx | 43. asdfgh |
| 4. qwerty | 14. football | 24. 123321 | 34. jordan | 44. buster |
| 5. 123456789 | 15. monkey | 25. 1234...890 | 35. jennifer | 45. andrew |
| 6. 12345 | 16. letmein | 26. p*s*y | 36. 123qwe | 46. batman |
| 7. 1234 | 17. shadow | 27. superman | 37. 121212 | 47. soccer |
| 8. 111111 | 18. master | 28. 270 | 38. killer | 48. tigger |
| 9. 1234567 | 19. 696969 | 29. 654321 | 39. trustno1 | 49. charlie |
| 10. dragon | 20. michael | 30. 1qaz2wsx | 40. hunter | 50. robert |

Password

Hashes cracked per second 4,005,900,000		
Length of password	Maximum number of possibilities	Length of time to crack
1	95	0 years, days, 0 hours, 0 minutes, 0 seconds
2	9,025	0 years, days, 0 hours, 0 minutes, 0 seconds
3	857,375	0 years, days, 0 hours, 0 minutes, 0 seconds
4	81,450,625	0 years, days, 0 hours, 0 minutes, 0 seconds
5	7,737,809,375	0 years, days, 0 hours, 0 minutes, 2 seconds
6	735,091,890,625	0 years, days, 0 hours, 3 minutes, 4 seconds
7	69,833,729,609,375	0 years, days, 5 hours, 51 minutes, 33 seconds
8	6,634,204,312,890,620	0 years, 19 days, 4 hours, 2 minutes, 48 seconds
9	630,249,409,724,609,000	5 years, 361 days, 23 hours, 52 minutes, 30 seconds
10	59,873,693,923,837,900,000	474 years, 345 days, 12 hours, 33 minutes, 54 seconds
11	5,688,000,922,764,600,000,000	45,025 years, 336 days, 17 hours, 6 minutes, 34 seconds
12	540,360,087,662,637,000,000,000	4,277,367 years, 138 days, 16 hours, 48 minutes, 15 seconds
13	51,334,208,327,950,500,000,000,000	406,349,901 years, 303 days, 13 hours, 55 minutes, 2 seconds
14	4,876,749,791,155,300,000,000,000,000	38,603,240,579 years, 273 days, 14 hours, 3 minutes, 40 seconds
15	463,291,230,159,753,000,000,000,000,000	3,667,307,854,981 years, 306 days, 22 hours, 26 minutes, 8 seconds

Counter Measures

Countermeasures - Technology and Defense



Mitigating Solutions Controls

HOW TO ACHIEVE CYBER RESILIENCE IN 7 STEPS



STEP 1 SYSTEM HYGIENE

Establish a proactive and systematic process for managing standard systems hygiene.



STEP 2 DEVELOP A PLAN

Create a cross-functional team of senior management to plan for cyber security events and consider hypothetical attacks.



STEP 3 MAP OUT RISK PROFILE

Study cyber patterns and attack modes to develop a tailored approach to protecting company assets.



STEP 4 ASSESS & MEASURE

Focus on rough figures, not precise estimates and avoid analysis paralysis.



STEP 5 MITIGATE RISK

Invest in risk mitigation measures to protect company assets at greatest risk.



STEP 6 CYBER INSURANCE

Obtain cyber insurance to provide contingent capital and specialized assistance in the event of an attack.



STEP 7 GET STARTED

A rough plan is okay – becoming resilient to cyber risk starts with a single step.

Indian Cyber Security Initiatives– Use Case

Å NISP 2013

Å NCIIPC

Å CERT-In

Å Sectorial Solutions

Å GST

Indian Cyber Security Initiatives– Use Case

Å Reserve Bank of India (RBI)

Å CERT-Fin

Å IDRBT

Å IRDAI

Å IT Act (A)2008

Å UIDAI

Å NPCI

Å SEBI

Thank you

Srinivas Bhoosarapu

Mail: srinivas.bhoosarapu@gmail.com

Mobile: +91 9849939719

WhatsApp: +91 9154035731

Activities in Workshop

Å Use Cases on Cyber Threats

Å Threat Finding Activity

Å Resolutions and Controls

Å Interactive session

Å Team based activity for complete cycle of PDCA on use case

Å Product Development on Cyber Liability parameter find in case Attack

Agenda

Å Insurance Cyber Risk

Å Core Insurance System & Data Breaches in Insurance System

Å Threats Land scape - Smart Cities, IoT, Critical Infrastructure, Banking Solutions, SCADA Systems, Power Grids, Data Centers, Human Resource Behavioral , Third party Motor Vehicle, Health Data, Metro Rails System, SMAC

Å Opportunities – Vulnerability Gap Assessment, Cyber Liability Insurance Products, Skill Development in Cyber Security Monitoring , SOC,NOC

Å Involvement C- Suite and Board in Cyber Risk Security.

Å Challenges – Assessment of Loss, Claim Analysis in disruption, Actuarial Analysis for New Product Development for Cyber Insurance

Å Indian Cyber Security Use Cases

Cyber Risk - Insurance

