NYU Leonard N. Stern School of Business
Master of Science Risk Management
RISK MANAGEMENT
SYMPOSIUM 2015

“Defending Against Cyber Security Threats to the Payment and Banking Systems”

Andrew Koh
Class of 2010 MSRM
Class of 2009 MSGF

LINKEDIN Profile:

https://sg.linkedin.com/in/andrewkohmw

Thought leader, speaker, moderator, panelist, writer, advisor

- Selected conferences: World Cards & Payments; Financial Times; RiskMinds Asia; Bloomberg; Cards & Payments Asia; The Asian Banker.
- Presented to central banks, regulators, government agencies, financial institutions, varsities, private equity & fin-tech firms.
- Published articles for award winning magazine: Strategic Risk Asia.

25 years in banking, finance, payment & cards sectors

- Experiences in Basel, ERM, GRC, Fraud, Outsourcing, RCSA, KRIs, Stress Testing, Incident Response, BCP, Audit frameworks & systems.
- Currently, he is the Deputy Chief Manager of Risk Control in China Construction Bank, S'pore. and was Vce President of ERM for NETS.

Avid Lifelong Learner

- Class of 2010 MS Risk Managment (Stern)
- Class of 2009 MS Global Finance (Stern + HKUST)

AGENDA

Part 1 - Cyber Security Threats

- High risk, high profile threats to payments & banking systems.
- Increasing sophistication and scale of threats.
- Defense and Attack Technologies
- Using data, analytics and intelligence to combat threats.
- Power of collaboration and the role of regulators.

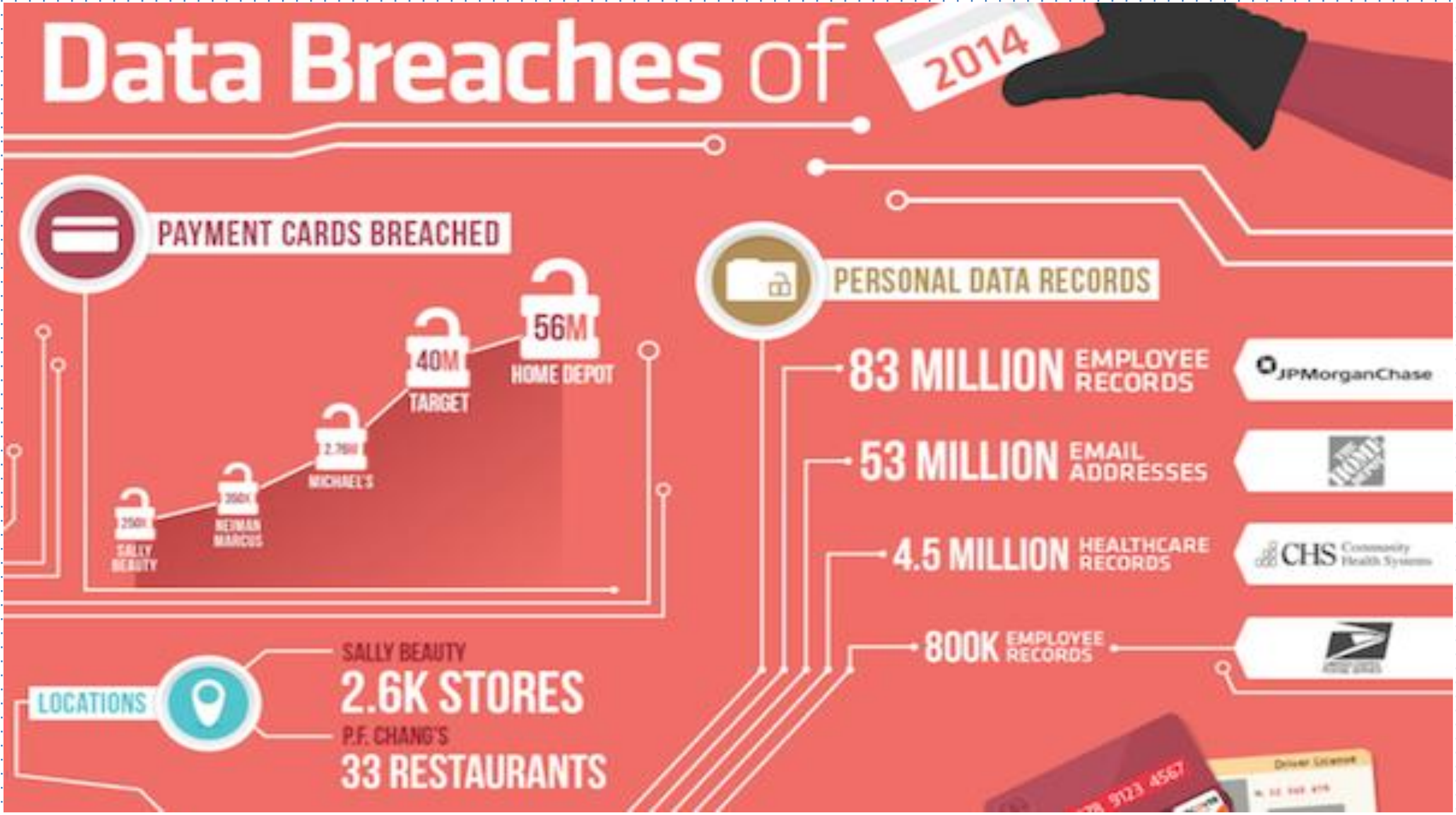
Part 2 - Defending against Cyber Threats/ORM Perspective

- Defining roles and responsibilities in cyber risk governance.
- Identifying and protecting information assets most important to your firm and susceptible to cyber threats.
- How can Key Risk Indicators (KRIs) effectively interact with other tools to monitor attempts of cyber-attacks?
- Interplay of Incident Response and Business Continuity planning.

Questions & Answers

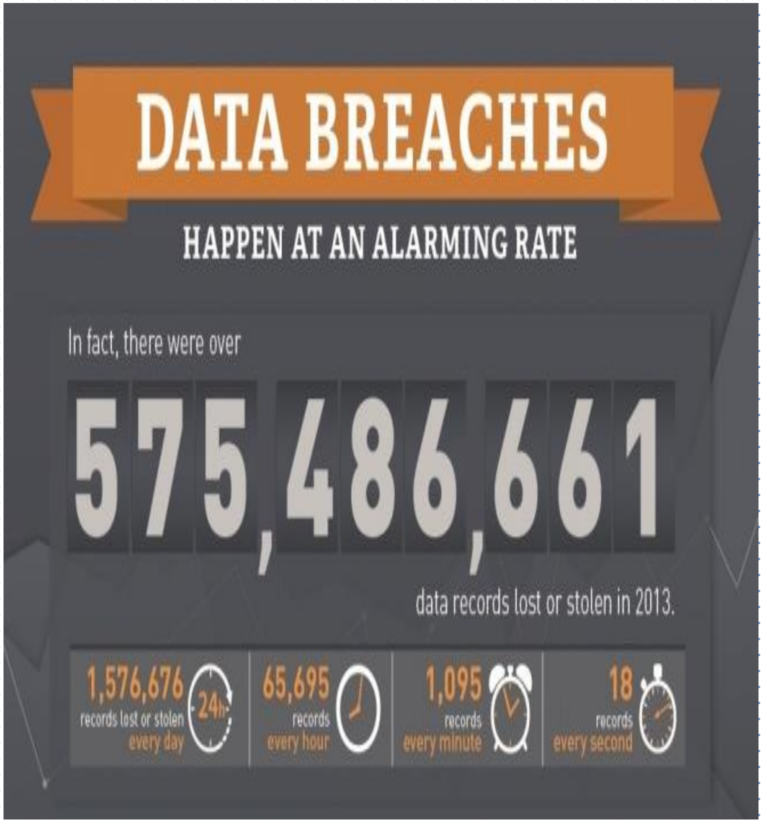
Part 1 - Cyber Security Threats

High risk, High profile threats to payments & banking systems.



High risk, High profile threats to payments & banking systems.

DATA IS THE NEW CURRENCY!



DATA BREACHES

HAPPEN AT AN ALARMING RATE

In fact, there were over

575,486,661

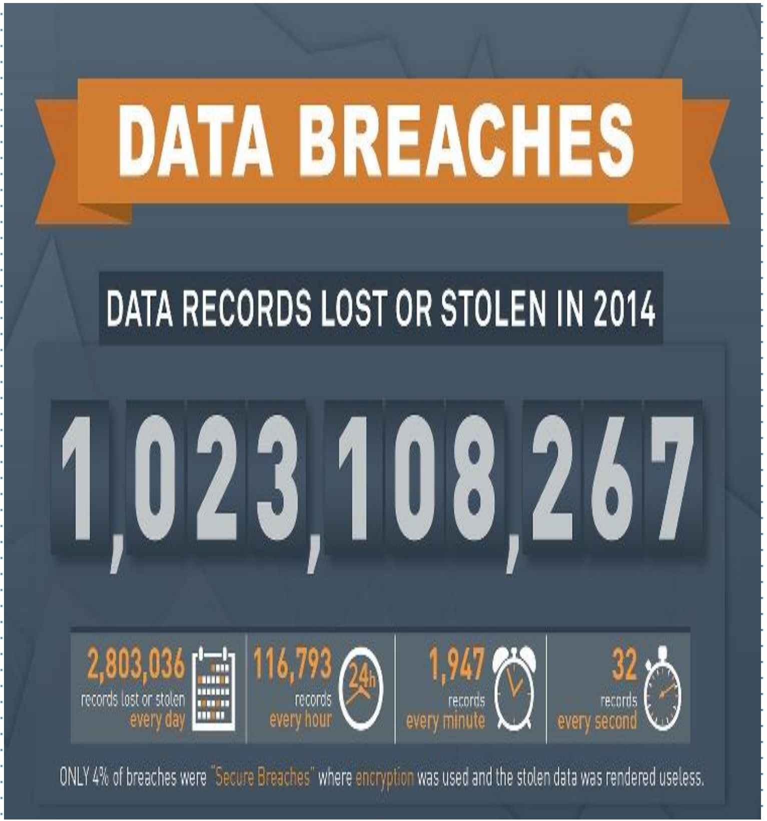
data records lost or stolen in 2013.

1,576,676 records lost or stolen every day

65,695 records every hour

1,095 records every minute

18 records every second



DATA BREACHES

DATA RECORDS LOST OR STOLEN IN 2014

1,023,108,267

2,803,036 records lost or stolen every day

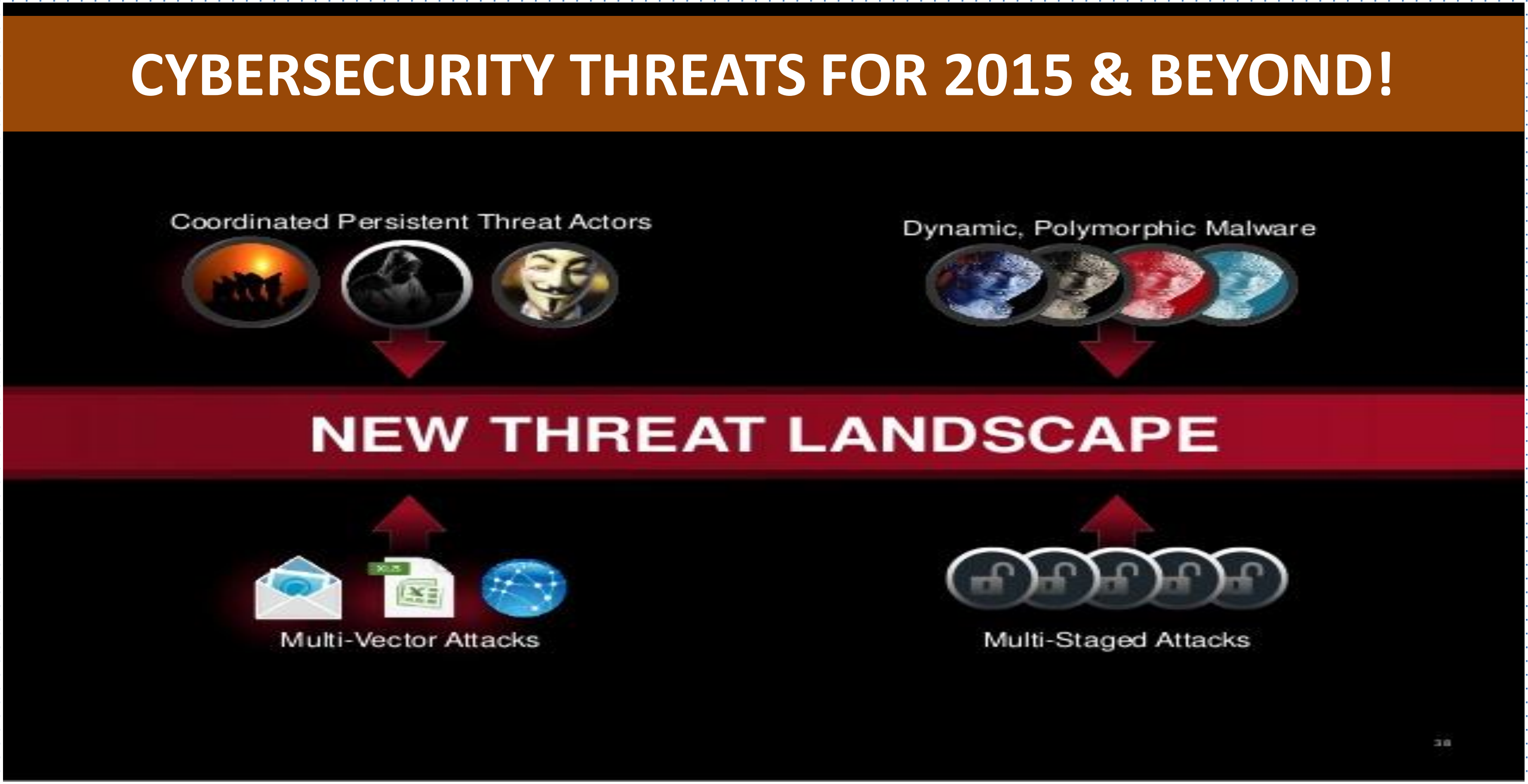
116,793 records every hour

1,947 records every minute

32 records every second

ONLY 4% of breaches were "Secure Breaches" where encryption was used and the stolen data was rendered useless.

High risk, High profile threats to payments & banking systems.



CYBERSECURITY THREATS FOR 2015 & BEYOND!

Coordinated Persistent Threat Actors

Dynamic, Polymorphic Malware

NEW THREAT LANDSCAPE

Multi-Vector Attacks

Multi-Staged Attacks

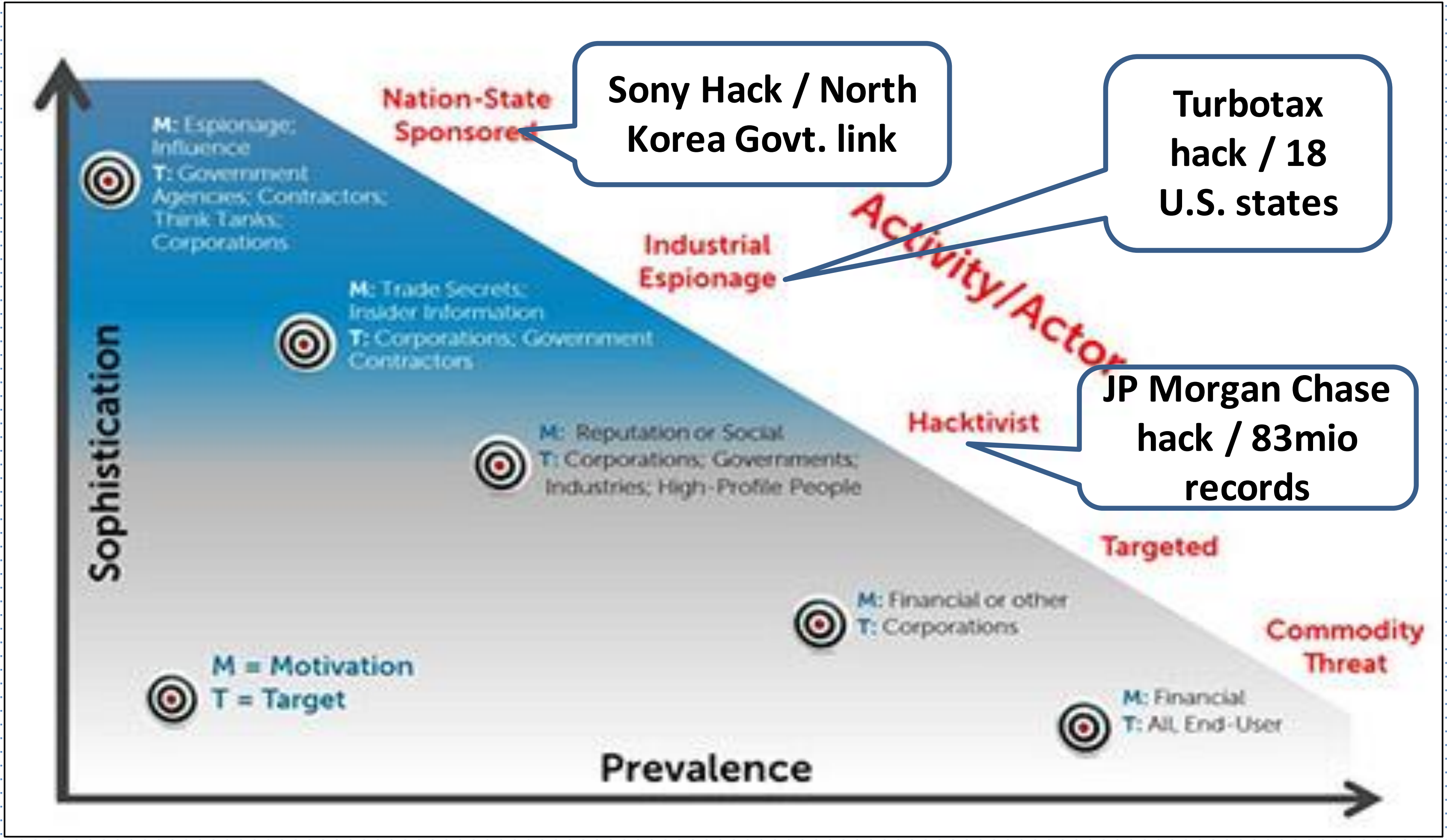
High risk, High profile threats to payments & banking ystems

Top 5 Threats Identified By NETS - Singapore national payment operator	
Cyber-Terrorist Groups	1
Politically motivated Groups	2
Hackers / Hacking Incidents	3
Cyber Loss Incidents	4
Payments Disruptions due to cyber-attacks and related incidents	5

High risk, High profile threats to payments & banking ystems

Top 5 Threats Identified CCB Singapore	
Cybercriminals and their actions	1
Insider Threats	2
Brand & Reputational risks	3
Non compliance to regulatory requirements on cybersecurity.	4
Business Disruptions	5

Increasing Sophistication & Scale of Threat

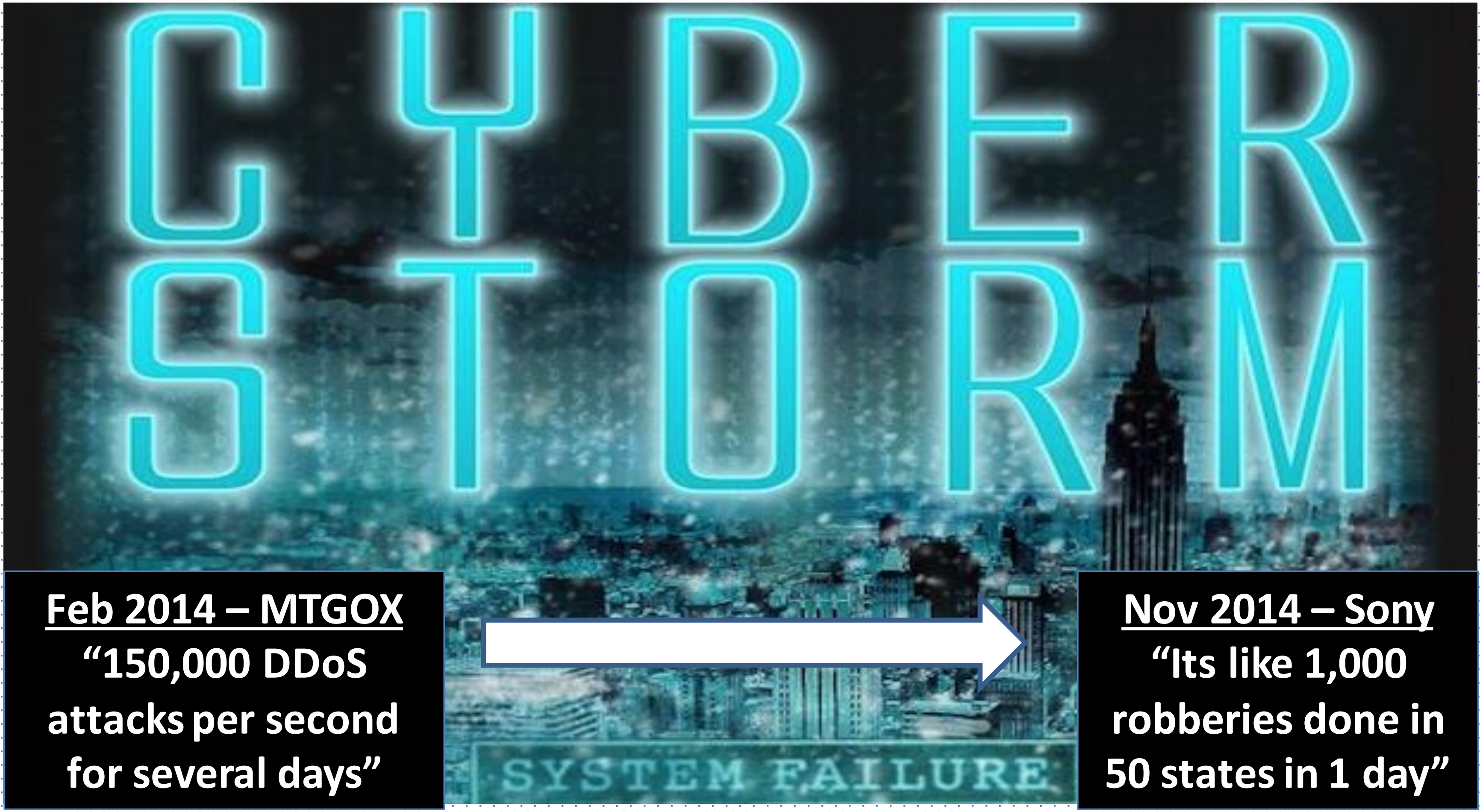


Sony Hack / North Korea Govt. link

Turbotax hack / 18 U.S. states

JP Morgan Chase hack / 83mio records

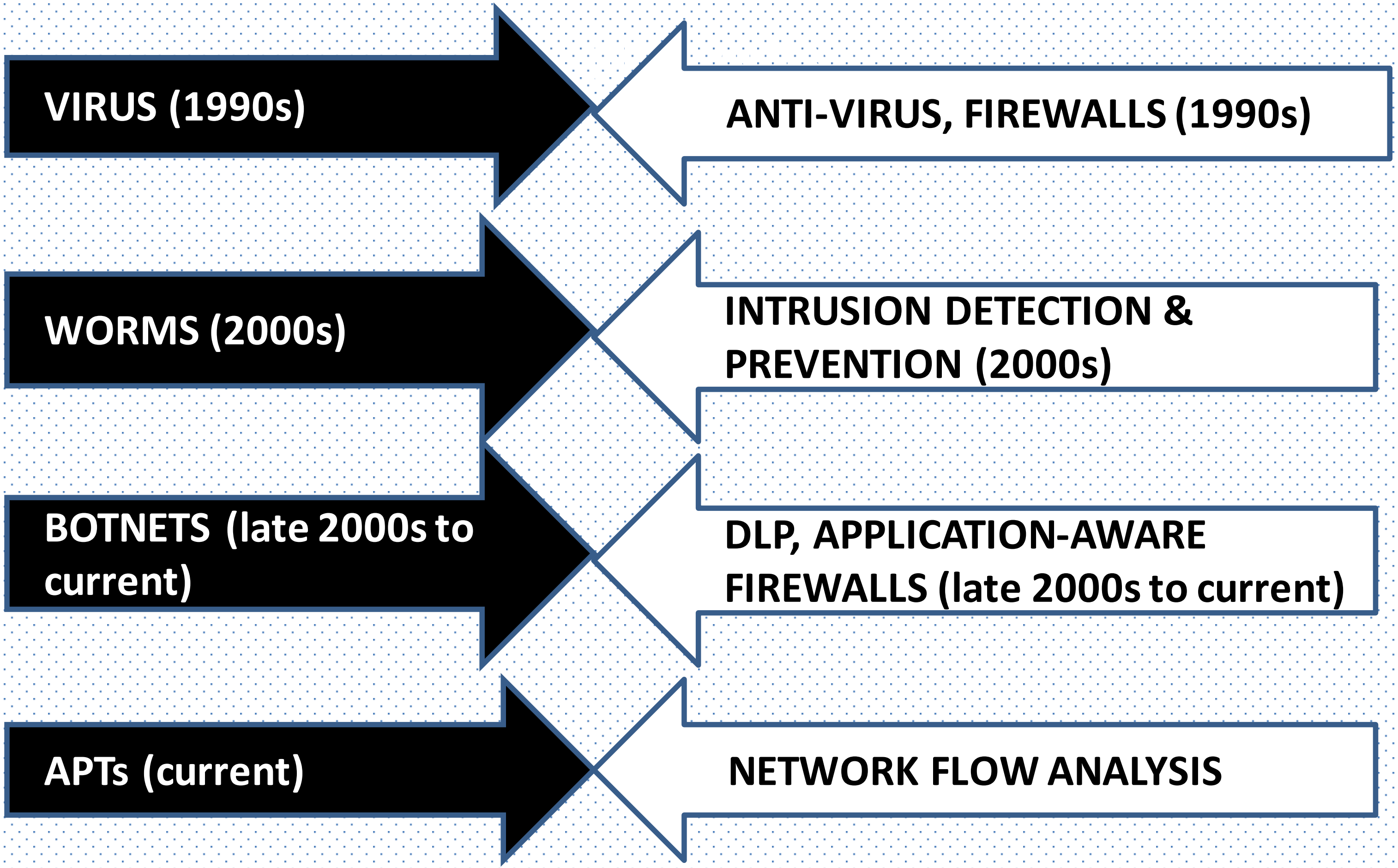
Increasing Sophistication & Scale of Threat(NETS & CCB S'pore)



Feb 2014 – MTGOX
“150,000 DDoS attacks per second for several days”

Nov 2014 – Sony
“Its like 1,000 robberies done in 50 states in 1 day”

Defense and Attack Technologies (NETS & CCB S'pore)



VIRUS (1990s)

ANTI-VIRUS, FIREWALLS (1990s)

WORMS (2000s)

INTRUSION DETECTION & PREVENTION (2000s)

BOTNETS (late 2000s to current)

DLP, APPLICATION-AWARE FIREWALLS (late 2000s to current)

APTs (current)

NETWORK FLOW ANALYSIS

Defense and Attack Technologies (NETS)

Top 5 Security Threat Defense Used by Organization (CISO) *(Source: CISCO Annual Security Report 2015)*	
Network security, firewalls , intrusion prevention	64%
Web security	62%
Email/messaging security	58%
Data Loss Prevention (DLP)	55%
Encryption/privacy/data protection	55%

Defense and Attack Technologies

Huge Gaps in Defense Technologies we use today

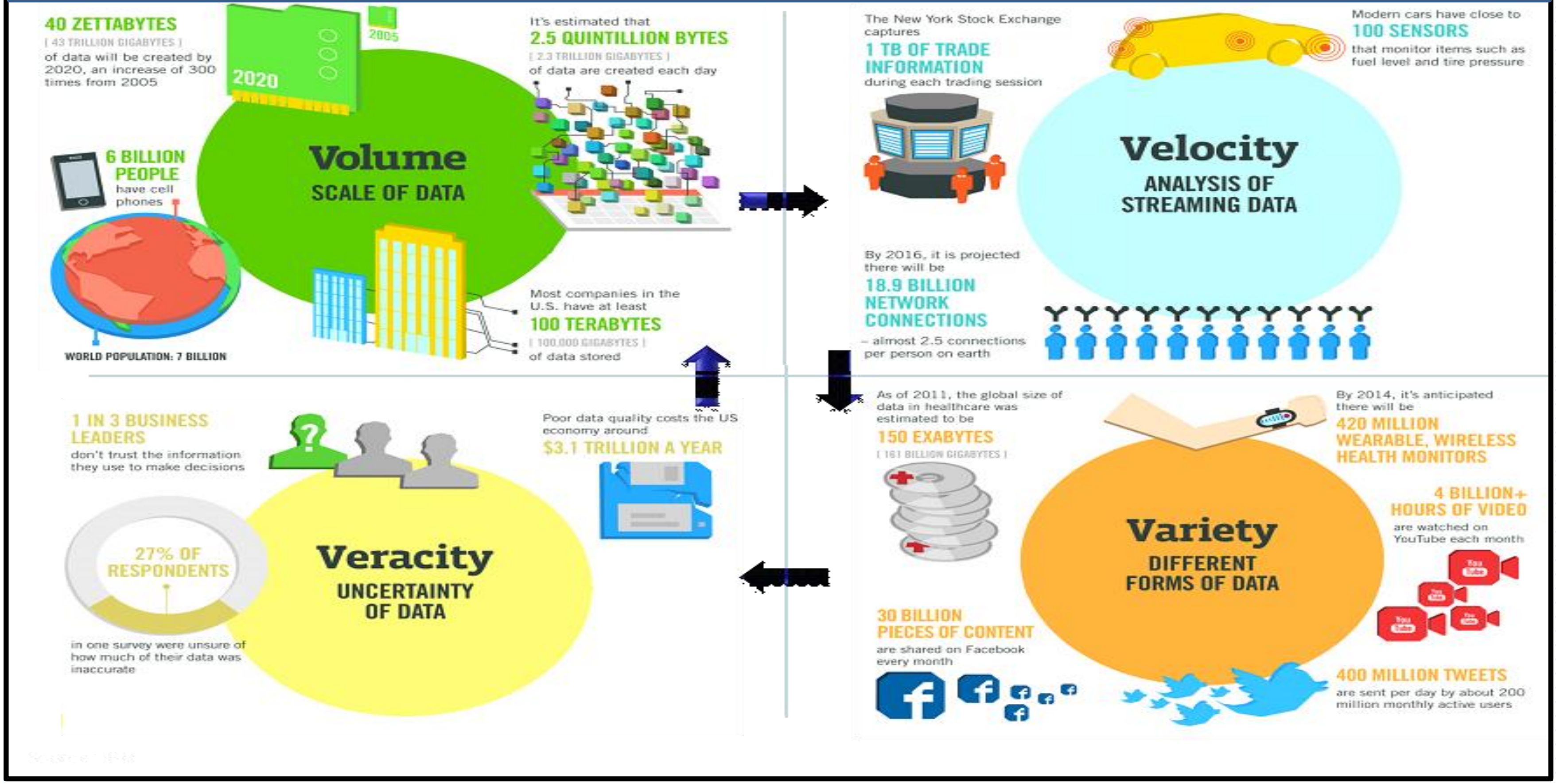
- Firms using yesterday‘s technologies to defend against cyber threats.
- Advances in technological innovations far exceeding security and risk management practices. Profits come first!
- There is a popular web-browser that can bypass firewalls w/o hacking.
- Lack of committed resources to defend against cyber-attacks.
- Most firms still view cyber threats as isolated, IT related issues.

Severe Knowledge Gaps in Cyber Risks & Security

- No skills and mindset for board of directors and C-Suite executives to make informed decisions.
- Lack of staff cybersecurity awareness to guard against cyber threats.

Using data, analytics and intelligence to combat threats(NETS)

BIG DATA



40 ZETTABYTES
[43 TRILLION GIGABYTES]
of data will be created by 2020, an increase of 300 times from 2005

6 BILLION PEOPLE have cell phones

WORLD POPULATION: 7 BILLION

It's estimated that **2.5 QUINTILLION BYTES** [2.3 TRILLION GIGABYTES] of data are created each day

Most companies in the U.S. have at least **100 TERABYTES** [100,000 GIGABYTES] of data stored

Volume
SCALE OF DATA

The New York Stock Exchange captures **1 TB OF TRADE INFORMATION** during each trading session

Modern cars have close to **100 SENSORS** that monitor items such as fuel level and tire pressure

Velocity
ANALYSIS OF STREAMING DATA

By 2016, it is projected there will be **18.9 BILLION NETWORK CONNECTIONS** – almost 2.5 connections per person on earth

1 IN 3 BUSINESS LEADERS don't trust the information they use to make decisions

Poor data quality costs the US economy around **$3.1 TRILLION A YEAR**

27% OF RESPONDENTS in one survey were unsure of how much of their data was inaccurate

Veracity
UNCERTAINTY OF DATA

As of 2011, the global size of data in healthcare was estimated to be **150 EXABYTES** [161 BILLION GIGABYTES]

By 2014, it's anticipated there will be **420 MILLION WEARABLE, WIRELESS HEALTH MONITORS**

4 BILLION+ HOURS OF VIDEO are watched on YouTube each month

Variety
DIFFERENT FORMS OF DATA

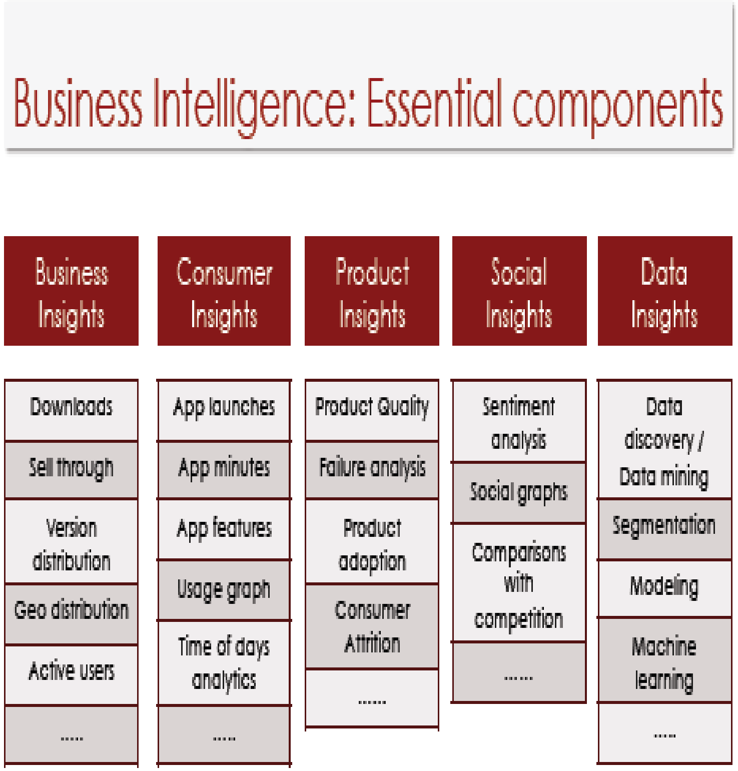
30 BILLION PIECES OF CONTENT are shared on Facebook every month

400 MILLION TWEETS are sent per day by about 200 million monthly active users

Source: IBM

Using data, analytics and intelligence to combat threats. (NETS)

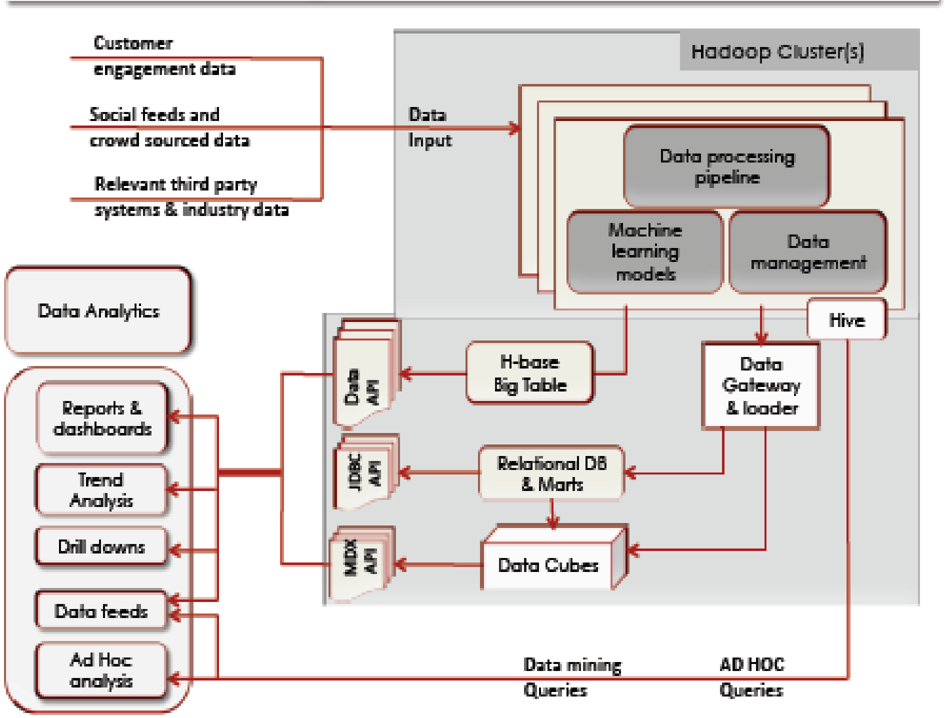
BIG DATA + BIZ INTELLIGENCE



Business Intelligence: Essential components

Business Insights	Consumer Insights	Product Insights	Social Insights	Data Insights
Downloads	App launches	Product Quality	Sentiment analysis	Data discovery / Data mining
Sell through	App minutes	Failure analysis	Social graphs	Segmentation
Version distribution	App features	Product adoption	Comparisons with competition	Modeling
Geo distribution	Usage graph	Consumer Attrition	……	Machine learning
Active users	Time of days analytics	……		…..
…..	…..			

BI Solution: Big Data Service



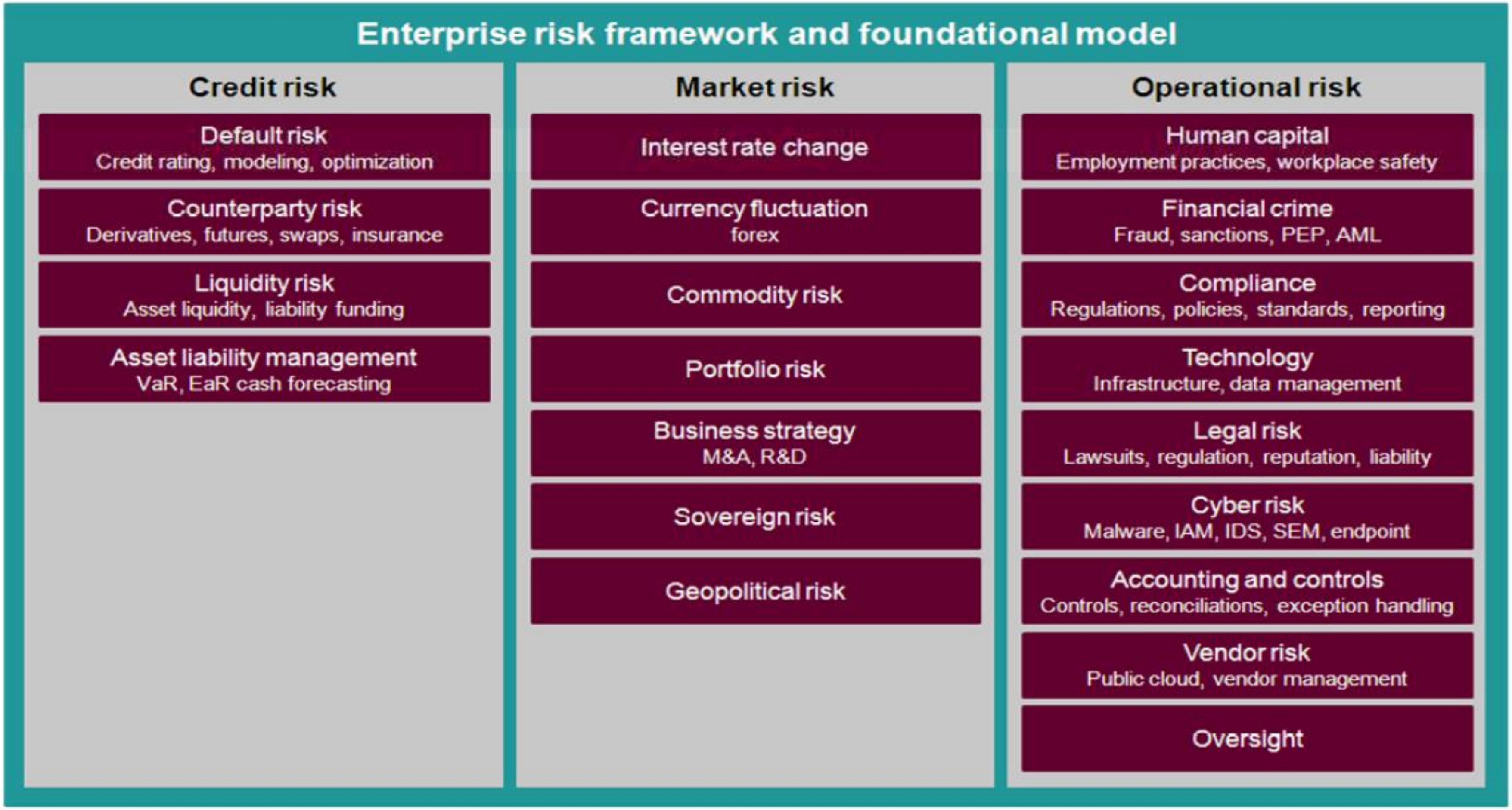
Power of collaboration and the role of regulators.. (NETS & CCB S'pore)

ANZ
POSB
Deutsche Bank
CIMBBANK
DBS
HSBC
citibank
Maybank
OCBC Bank
遠東國際商業銀行
Far Eastern Int'l Bank
RHB
UOB
大華銀行
RBS
The Royal Bank of Scotland
Standard Chartered
SMBC
NETS
a better way to pay
VISA
MasterCard
eNETS
UnionPay
银联
UnionPay International
ez-link
AXS
paikia.com
PayPal
epins
A service by Card Alliance
AMERICAN EXPRESS
dash
CREATED BY SINGTEL AND STANDARD CHARTERED
WESTERN UNION
MONEY TRANSFER

Power of collaboration and the role of regulators.

Part 2 - Defending against Cyber Threats from an Operational Risk Manager's Perspective.

Defining roles and responsibilities in cyber risk governance.



Enterprise risk framework and foundational model

Credit risk

- Default risk
  Credit rating, modeling, optimization
- Counterparty risk
  Derivatives, futures, swaps, insurance
- Liquidity risk
  Asset liquidity, liability funding
- Asset liability management
  VaR, EaR cash forecasting

Market risk

- Interest rate change
- Currency fluctuation
  forex
- Commodity risk
- Portfolio risk
- Business strategy
  M&A, R&D
- Sovereign risk
- Geopolitical risk

Operational risk

- Human capital
  Employment practices, workplace safety
- Financial crime
  Fraud, sanctions, PEP, AML
- Compliance
  Regulations, policies, standards, reporting
- Technology
  Infrastructure, data management
- Legal risk
  Lawsuits, regulation, reputation, liability
- Cyber risk
  Malware, IAM, IDS, SEM, endpoint
- Accounting and controls
  Controls, reconciliations, exception handling
- Vendor risk
  Public cloud, vendor management
- Oversight

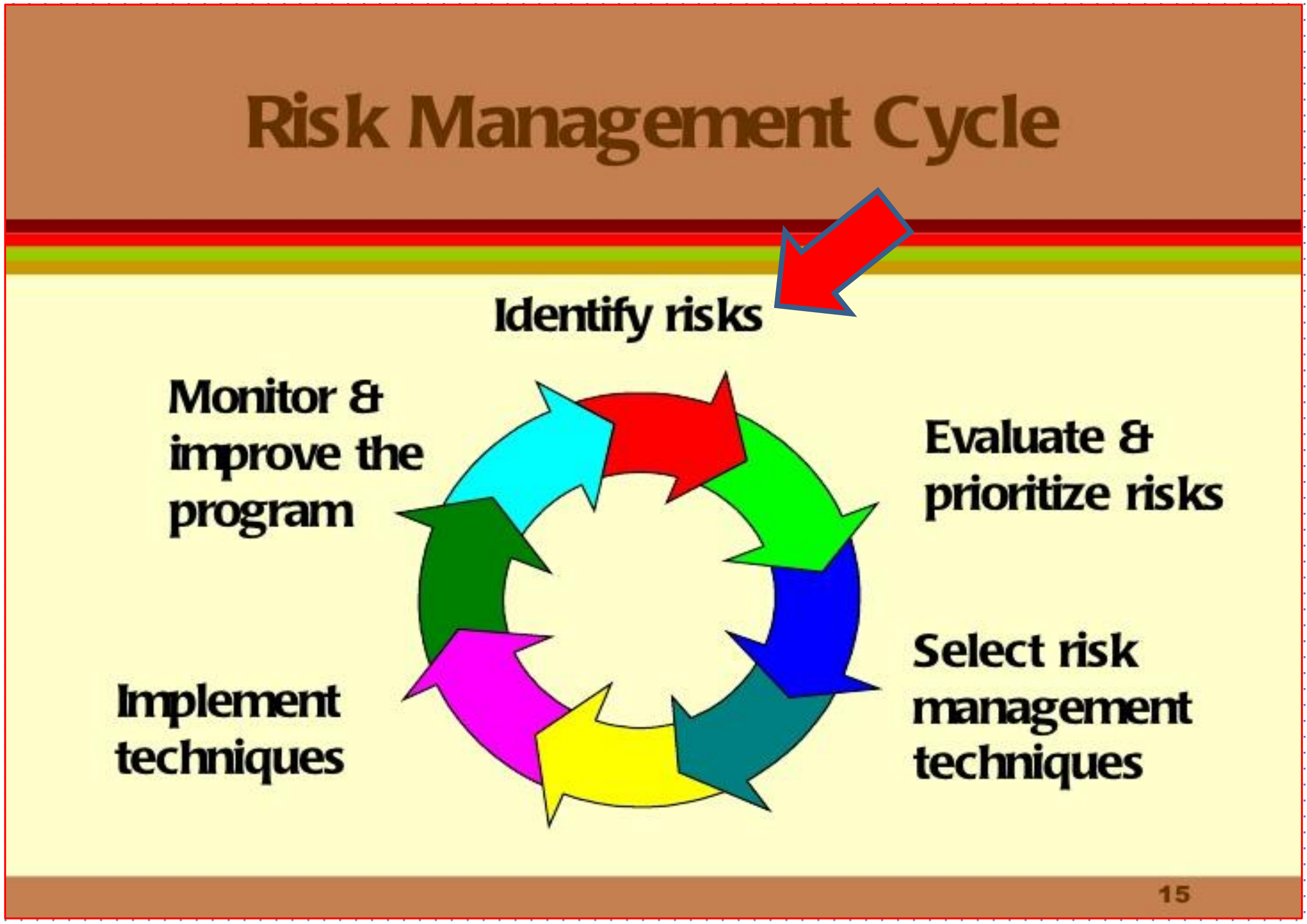
Source: IDC Financial Insights, 2011

Defining roles and responsibilities in cyber risk governance. (NETS & CCB S'pore)

Board of directors	Responsible for cyber risk framework.
Senior Management	Responsible for implementation and daily management of cyber risk framework.
Cyber Risk & Security Committee	Comprises of ORM, ERM, ITRM, Tech Ops, General Ops, BCM, Legal, Compliance, Audit (advisory).
Cyber Risk Champions (Biz & Support Units)	• Cyber risk identification & assessment. • Raise cyber risk warning alerts and recommend solutions to issues raised.

Identifying and protecting information assets most important to your firm and susceptible to cyber threats. (NETS ERM)

Strong Risk Culture



Risk Management Cycle

Identify risks

Evaluate & prioritize risks

Select risk management techniques

Implement techniques

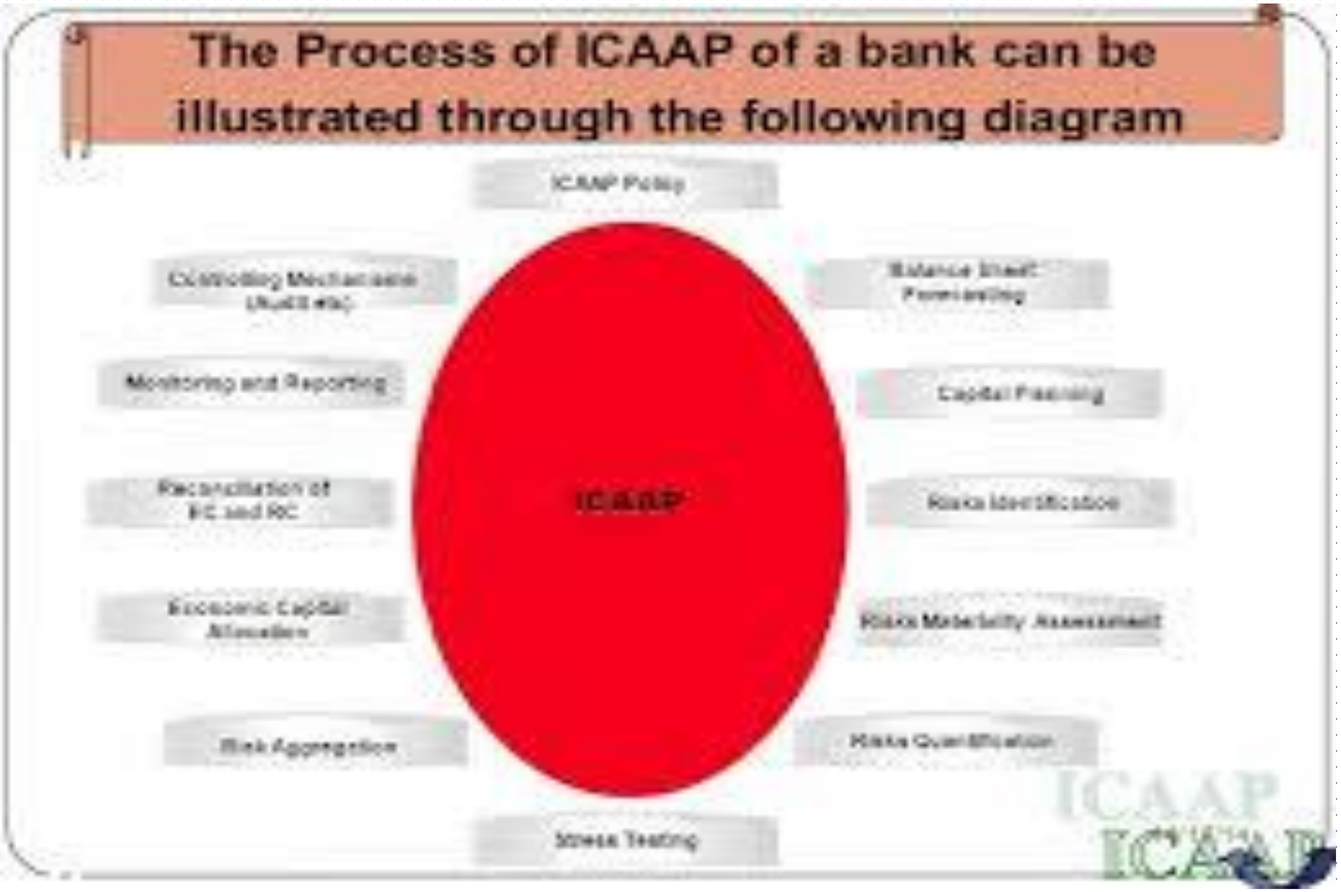
Monitor & improve the program

15

Cyber Risk Governance

Identifying and protecting information assets most important to your firm and susceptible to cyber threats. (CCB S'pore)

Strong Risk Culture



The Process of ICAAP of a bank can be illustrated through the following diagram

ICAAP Policy
Controlling Mechanisms (Audit etc)
Balance Sheet Forecasting
Monitoring and Reporting
Capital Planning
Reconciliation of EC and RC
ICAAP
Risks Identification
Economic Capital Allocation
Risks Materiality Assessment
Risk Aggregation
Risks Quantification
Stress Testing
ICAAP
ICAAP

Cyber Risk Governance

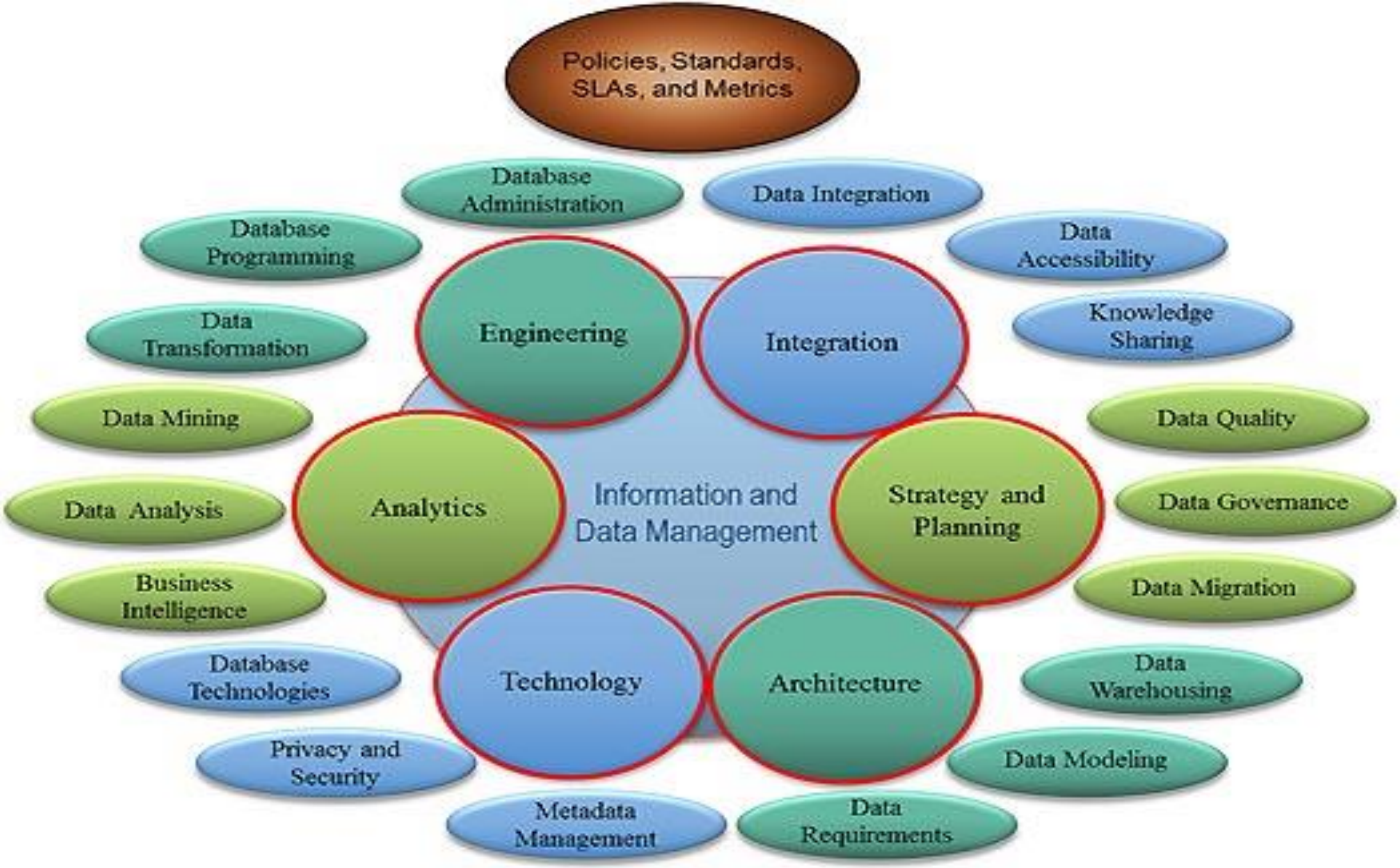
Identifying and protecting information assets most important to your firm and susceptible to cyber threats. (NETS & CCB S'pore)

Criteria Used	Risk Tools	Risk Impacts
Definition	Risk Strategies Selection	Dependent on whether it's data or assets or both.
Single Point of Failures	Process Mapping + RCSA	Failure at a single vector resulting in severe business disruptions/penalties, etc
Most Vulnerable Attack Surface Area	Cyber Security & Risk Assessment	Success rate of cyber attacks can lead to brand & reputational risks for firms.

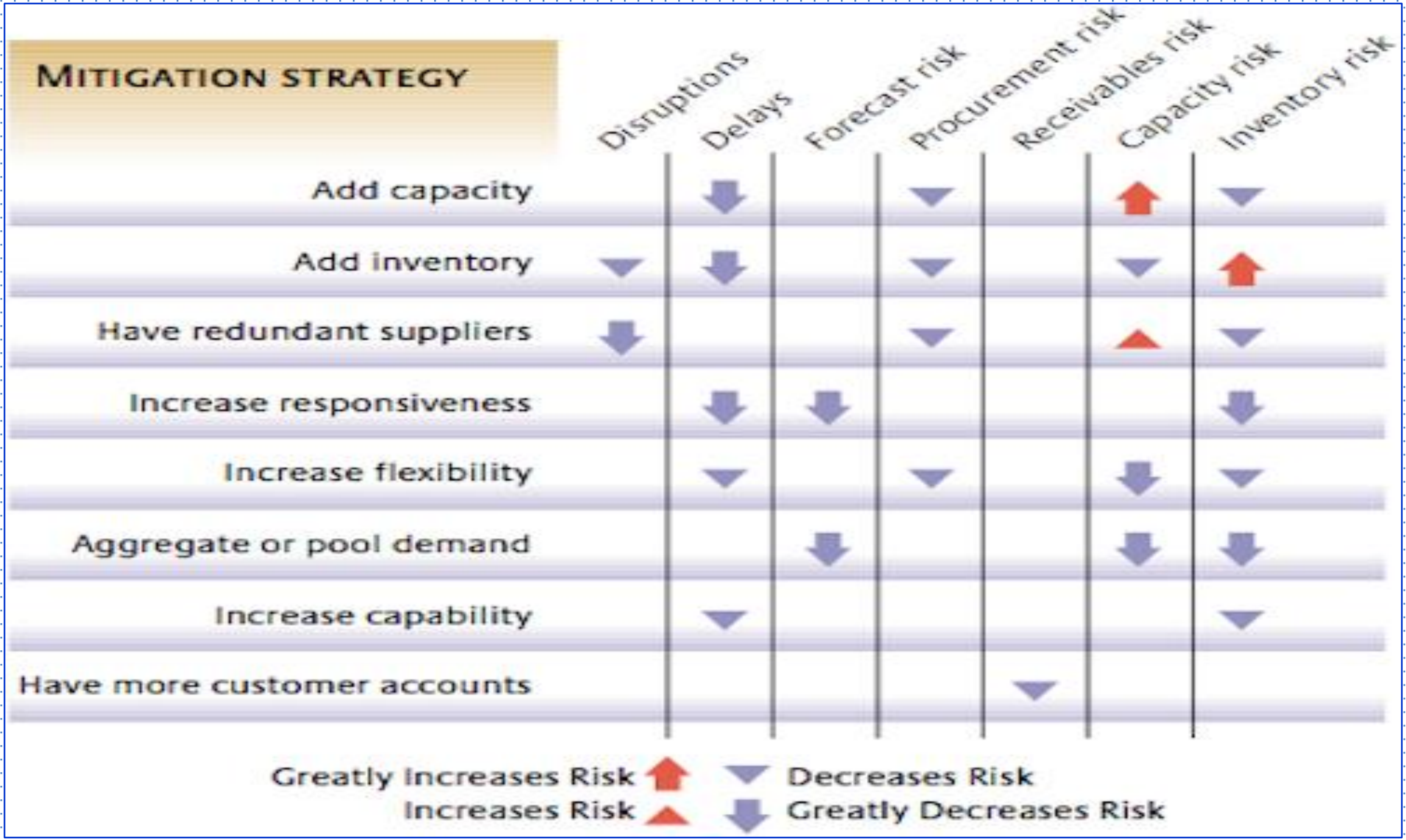
Definition of Information Assets (NETS)

Components	Protection Technologies
DATA	Data Encryption
APPLICATION	Application Hardening; Anti-virus
HOST	Authentication; Update Mgmt
INTERNAL NETWORK	Network Segmentation; IPSec; Network IDS.
PHYSICAL SECURITY	Guards; Locks; Tracking Devices
POLICIES, PROCEDURES & AWARENESS	User Education & Training

Definition of Information Assets (CCB S'pore)



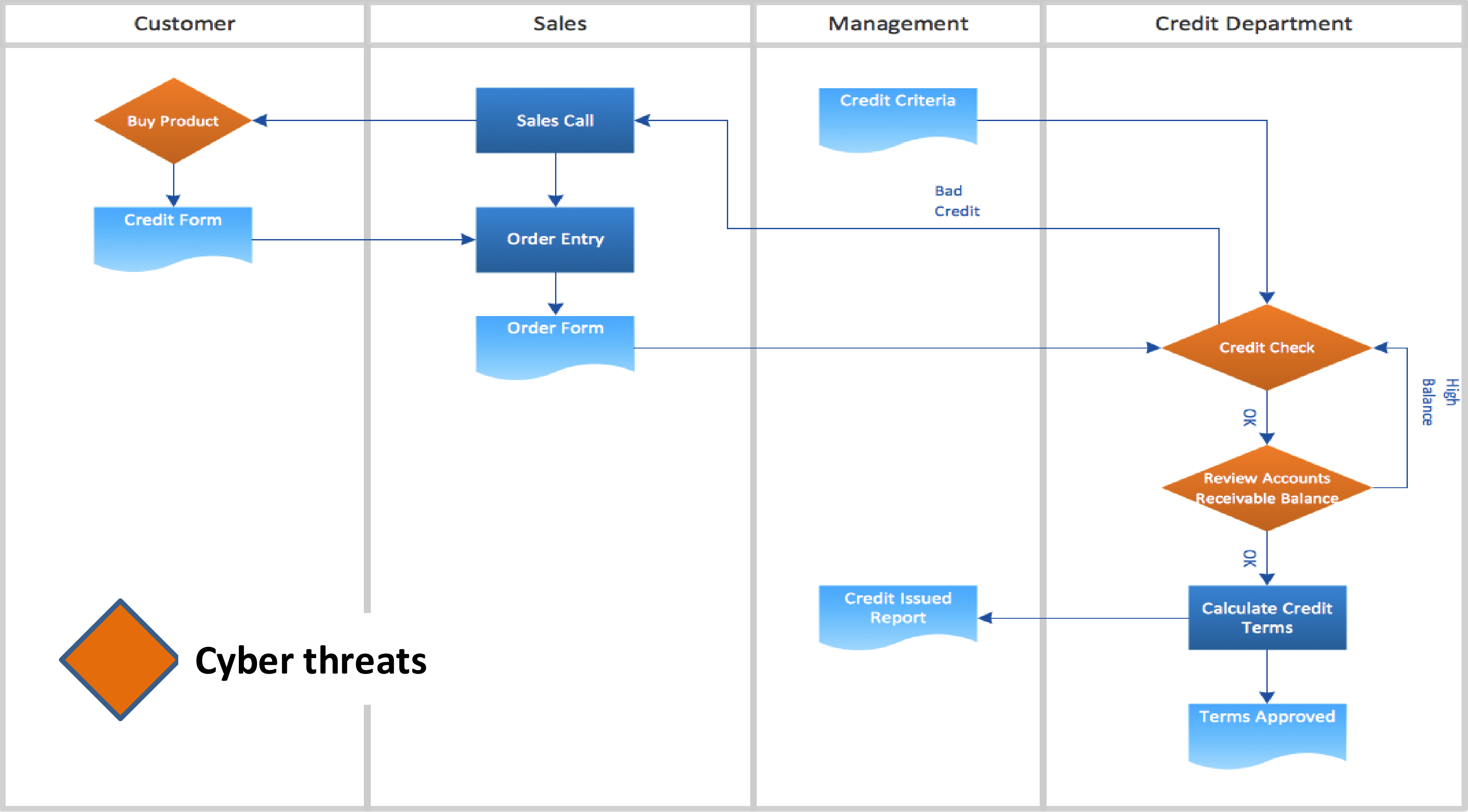
Definition & Risk Strategies Selection (NETS)



Mitigation strategy	Disruptions	Delays	Forecast risk	Procurement risk	Receivables risk	Capacity risk	Inventory risk
Add capacity		⬇		▼		⬆	▼
Add inventory	▼	⬇		▼		▼	⬆
Have redundant suppliers	⬇			▼		▲	▼
Increase responsiveness		⬇	⬇				⬇
Increase flexibility		▼		▼		⬇	▼
Aggregate or pool demand			⬇			⬇	⬇
Increase capability		▼					▼
Have more customer accounts					▼		

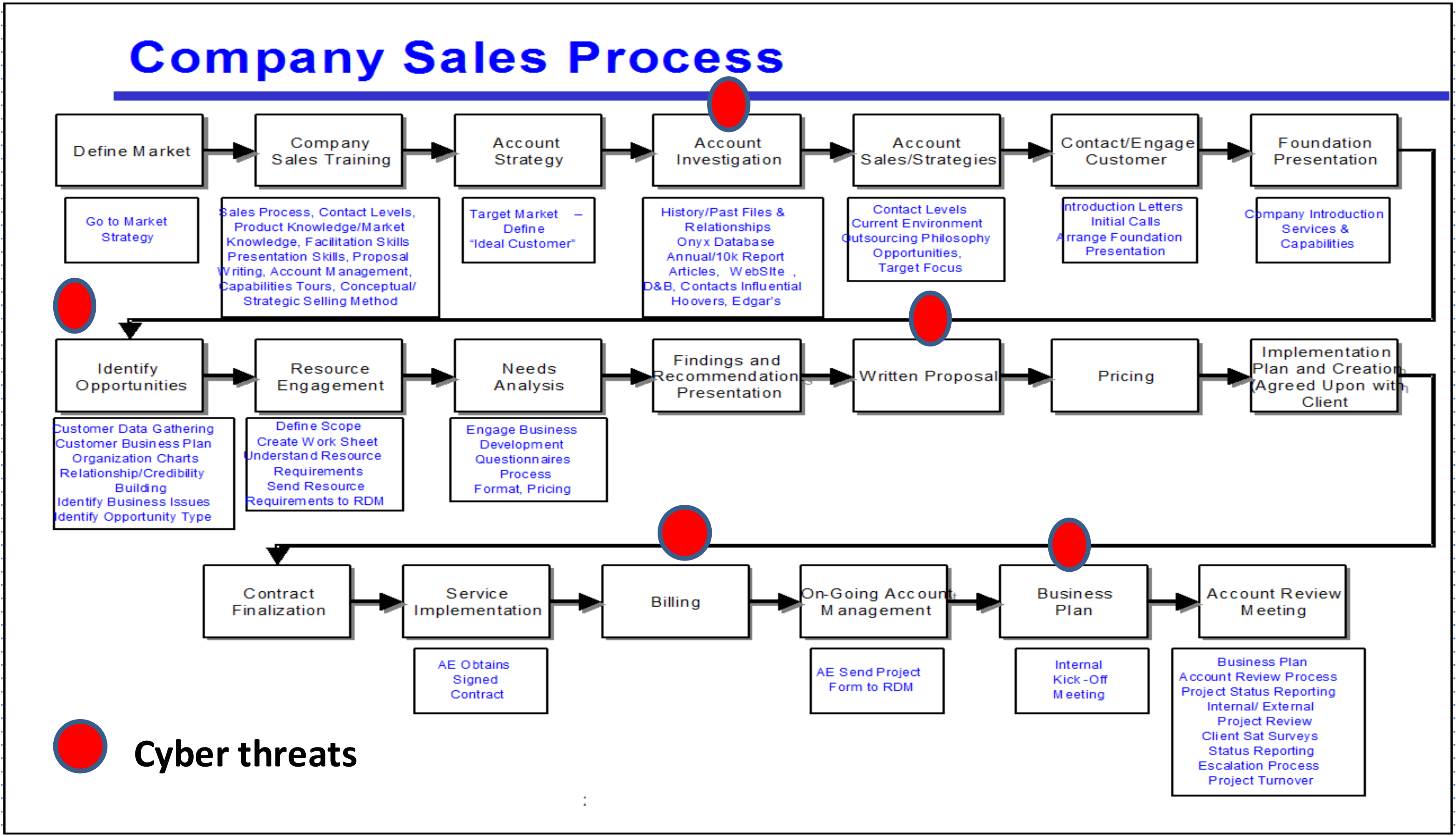
Greatly Increases Risk ⬆ ▼ Decreases Risk
Increases Risk ▲ ⬇ Greatly Decreases Risk

Single Point of Failure
END-TO-END PROCESS MAPPING (Level 1)



🔶 Cyber threats

Single Point of Failures
END-TO-END PROCESS MAPPING (Level 2)



Company Sales Process

Define Market
- Go to Market Strategy

Company Sales Training
- Sales Process, Contact Levels, Product Knowledge/Market Knowledge, Facilitation Skills Presentation Skills, Proposal Writing, Account Management, Capabilities Tours, Conceptual/ Strategic Selling Method

Account Strategy
- Target Market – Define "Ideal Customer"

● Account Investigation
- History/Past Files & Relationships Onyx Database Annual/10k Report Articles, WebSIte , D&B, Contacts Influential Hoovers, Edgar's

Account Sales/Strategies
- Contact Levels Current Environment Outsourcing Philosophy Opportunities, Target Focus

Contact/Engage Customer
- Introduction Letters Initial Calls Arrange Foundation Presentation

Foundation Presentation
- Company Introduction Services & Capabilities

● Identify Opportunities
- Customer Data Gathering Customer Business Plan Organization Charts Relationship/Credibility Building Identify Business Issues Identify Opportunity Type

Resource Engagement
- Define Scope Create Work Sheet Understand Resource Requirements Send Resource Requirements to RDM

Needs Analysis
- Engage Business Development Questionnaires Process Format, Pricing

Findings and Recommendations Presentation

● Written Proposal

Pricing

Implementation Plan and Creation (Agreed Upon with Client

Contract Finalization

Service Implementation
- AE Obtains Signed Contract

● Billing

On-Going Account Management
- AE Send Project Form to RDM

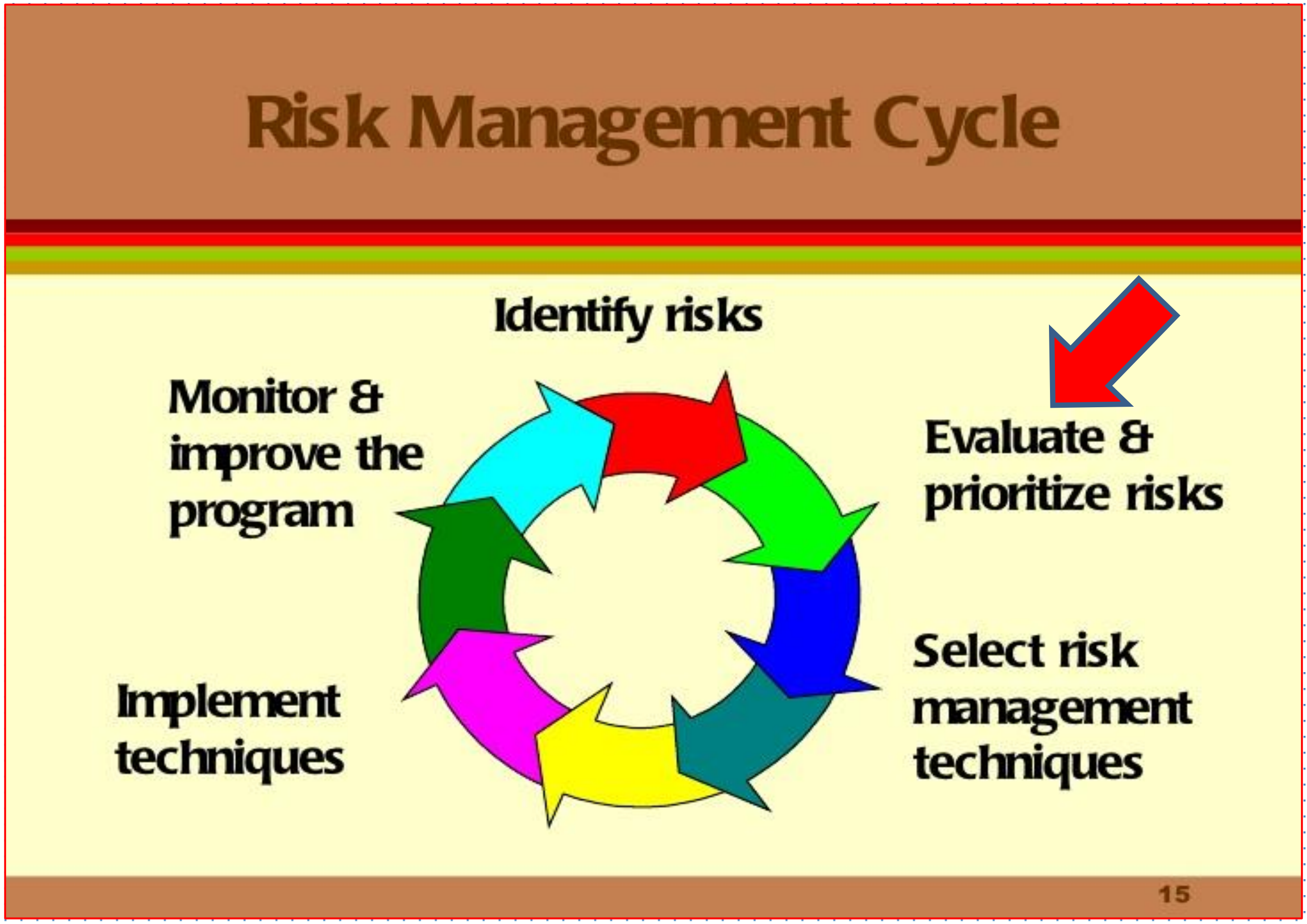
● Business Plan
- Internal Kick-Off Meeting

Account Review Meeting
- Business Plan Account Review Process Project Status Reporting Internal/ External Project Review Client Sat Surveys Status Reporting Escalation Process Project Turnover

● **Cyber threats**

Identifying and protecting information assets most important to your firm and susceptible to cyber threats.

Strong Risk Culture



Risk Management Cycle

Identify risks

Evaluate & prioritize risks

Select risk management techniques

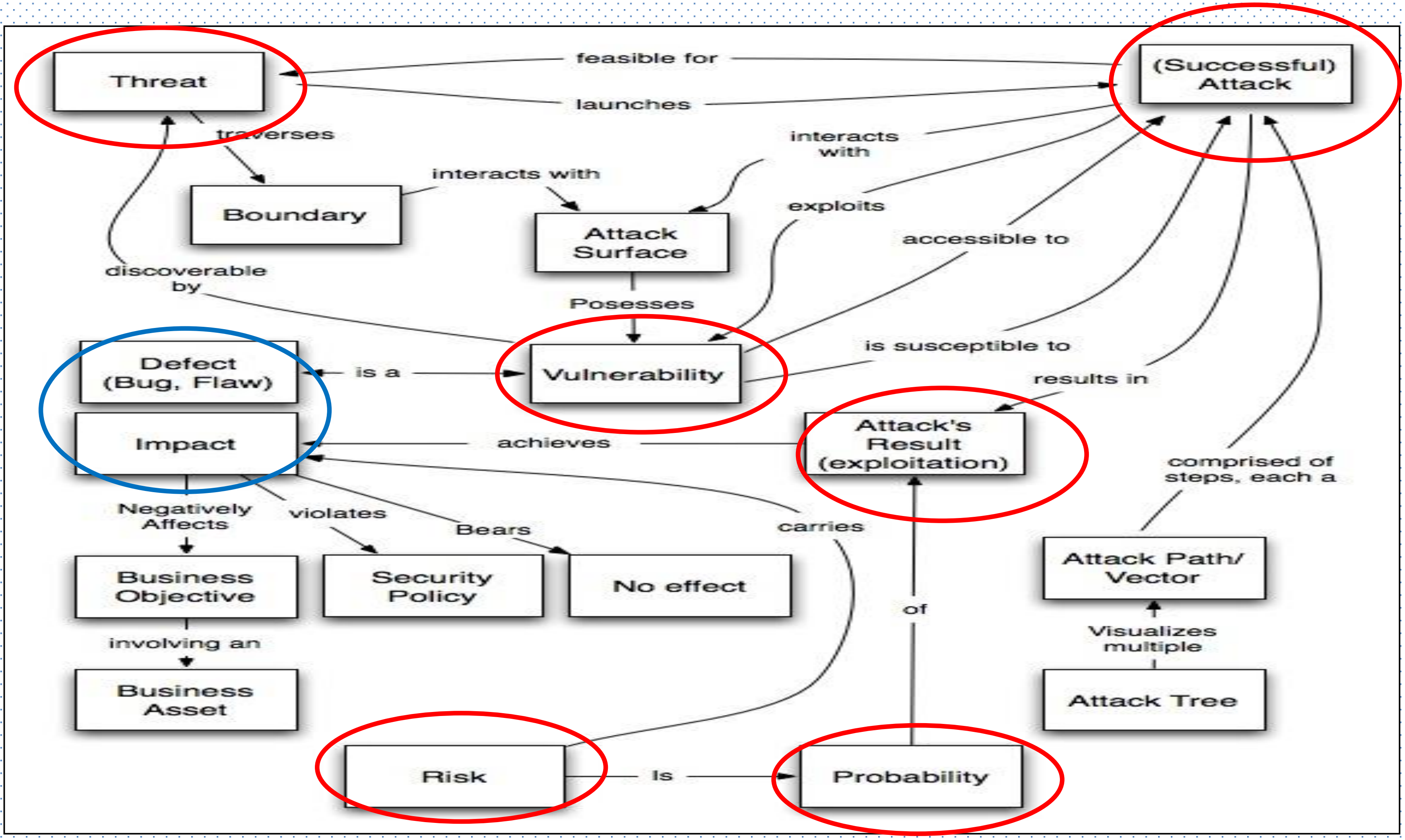
Implement techniques

Monitor & improve the program

15

Cyber Risk Governance

Cyber Security & Risk Assessment (Scenario Based Approach)

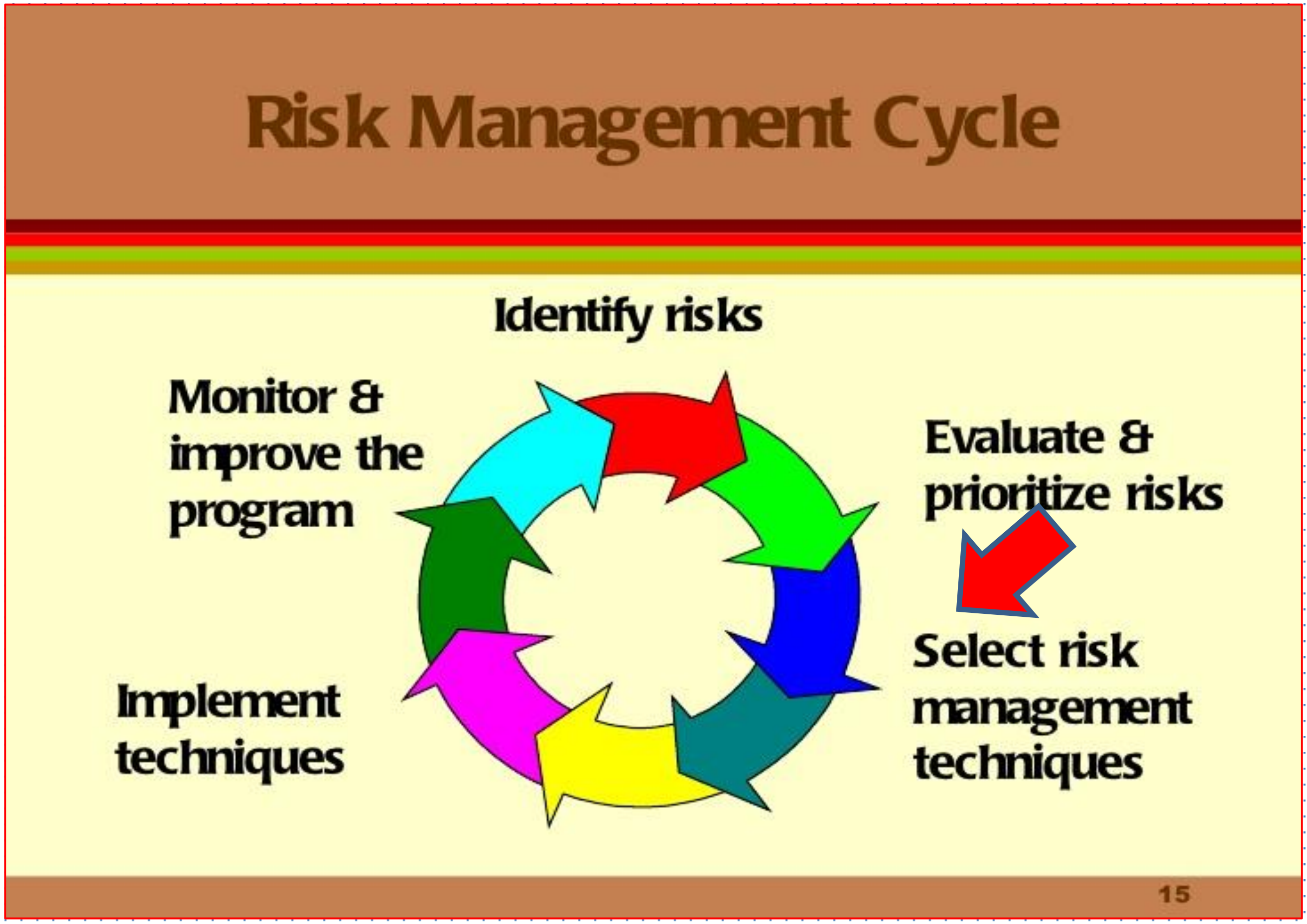


RISK & CONTROL SELF ASSESSMENT

Risk ~~Description~~ Identification	Risk Assessment										Risk Control Register	
	Gross Risk					Residual Risk						
	Likeli-hood	Impact	Gross Risk Score	Gross Risk Ranking	Gross Risk Rating	Likeli hood	Impact	Residual Risk Score	Residual Risk Ranking	Residual Risk Rating		
1. Economic												
Financial loss	3	3	9	1	1	2	2	4	1	1		
Transaction Value	2	3	4	2	2	1	2	2	2	2		
2. Operational												
System Availability	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
Staff Attrition	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
3. Brand and Reputation												
Damage to reputation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
4. Regulatory												
Non-compliance	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
5. Client												
Customer Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
Merchant Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		

Identifying and protecting information assets most important to your firm and susceptible to cyber threats.

Strong Risk Culture



Risk Management Cycle

Identify risks

Evaluate & prioritize risks

Select risk management techniques

Implement techniques

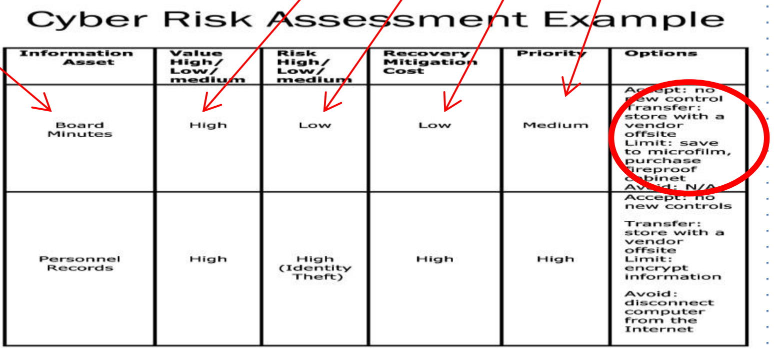
Monitor & improve the program

15

Cyber Risk Governance

RISK & CONTROL SELF ASSESSMENT

Risk ~~Description~~ Identification	Risk Assessment										Risk Control Register	
	Gross Risk					Residual Risk						
	Likeli-hood	Impact	Gross Risk Score	Gross Risk Ranking	Gross Risk Rating	Likeli hood	Impact	Residual Risk Score	Residual Risk Ranking	Residual Risk Rating		
1. Economic												
Financial loss	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
Transaction Value	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
2. Operational												
System Availability	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
Staff Attrition	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
3. Brand and Reputation												
Damage to reputation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
4. Regulatory												
Non-compliance	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
5. Client												
Customer Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		
Merchant Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA		

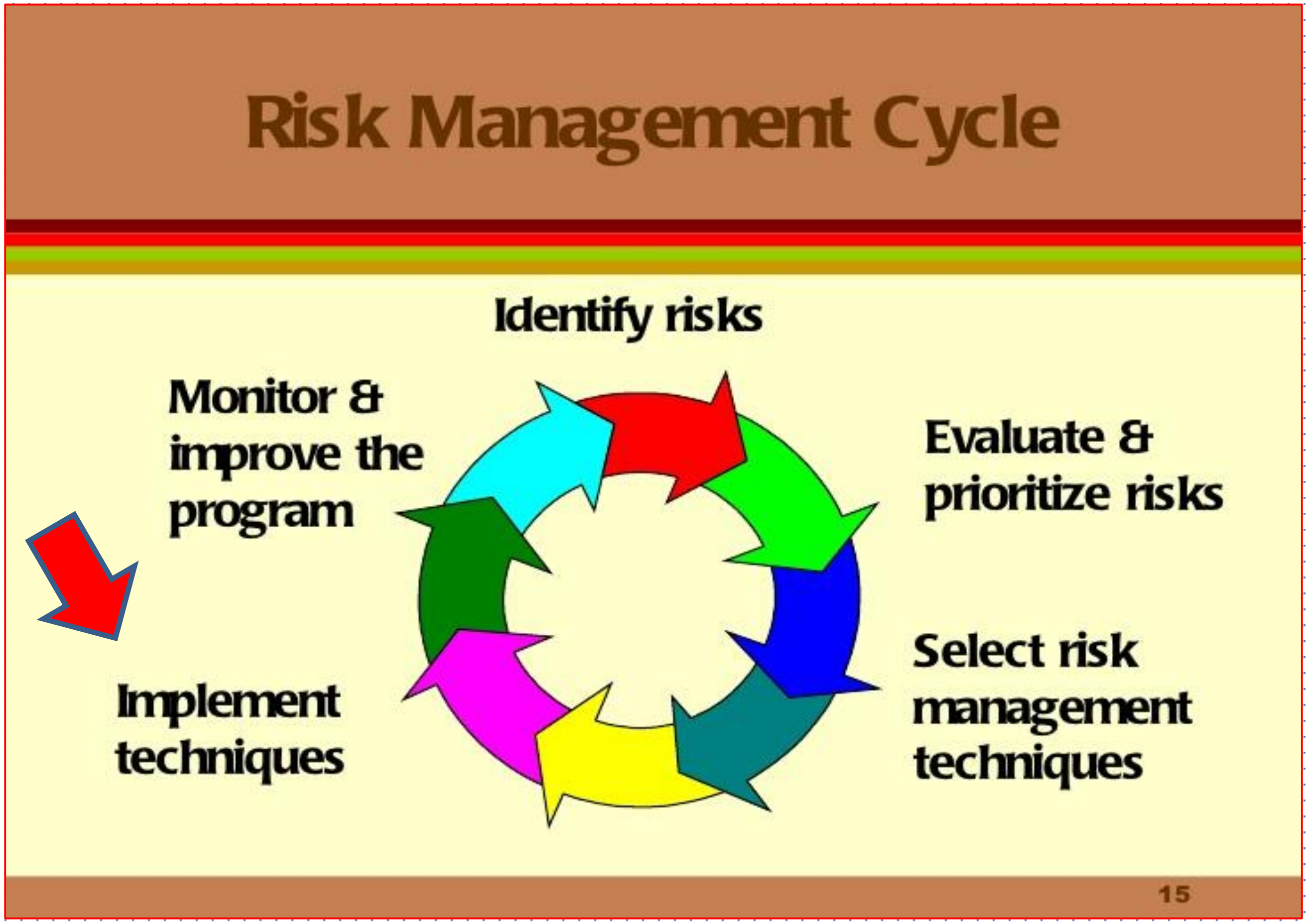


Cyber Risk Assessment Example

Information Asset	Value High/ Low/ medium	Risk High/ Low/ medium	Recovery Mitigation Cost	Priority	Options
Board Minutes	High	Low	Low	Medium	Accept: no new control Transfer: store with a vendor offsite Limit: save to microfilm, purchase fireproof cabinet Avoid: N/A
Personnel Records	High	High (Identity Theft)	High	High	Accept: no new controls Transfer: store with a vendor offsite Limit: encrypt information Avoid: disconnect computer from the Internet

Identifying and protecting information assets most important to your firm and susceptible to cyber threats.

Strong Risk Culture



Risk Management Cycle

Identify risks

Evaluate & prioritize risks

Select risk management techniques

Implement techniques

Monitor & improve the program

15

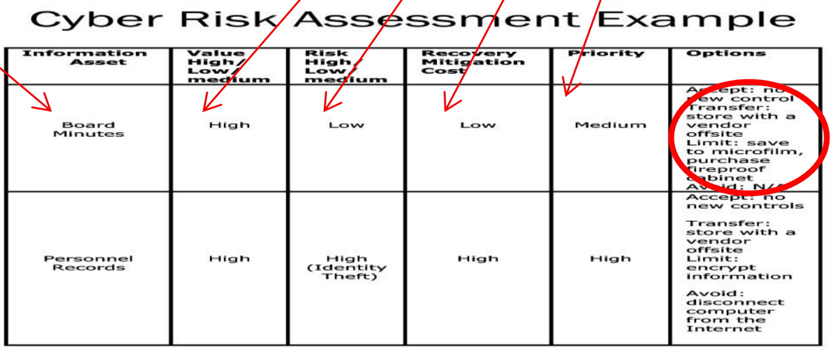
Cyber Risk Governance

RISK & CONTROL SELF ASSESSMENT

Risk ~~Description~~ Identification	Risk Assessment										Risk Control Register
	Gross Risk					Residual Risk					
	Likeli-hood	Impact	Gross Risk Score	Gross Risk Ranking	Gross Risk Rating	Likeli hood	Impact	Residual Risk Score	Residual Risk Ranking	Residual Risk Rating	Effective Controls in place? (Y/N)
1. Economic											
Financial loss	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Transaction Value	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
2. Operational											
System Availability	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Staff Attrition	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
3. Brand and Reputation											
Damage to reputation	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
4. Regulatory											
Non-compliance	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
5. Client											
Customer Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	
Merchant Impact	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	

Key Risk Indicators

Review KRI Thresholds



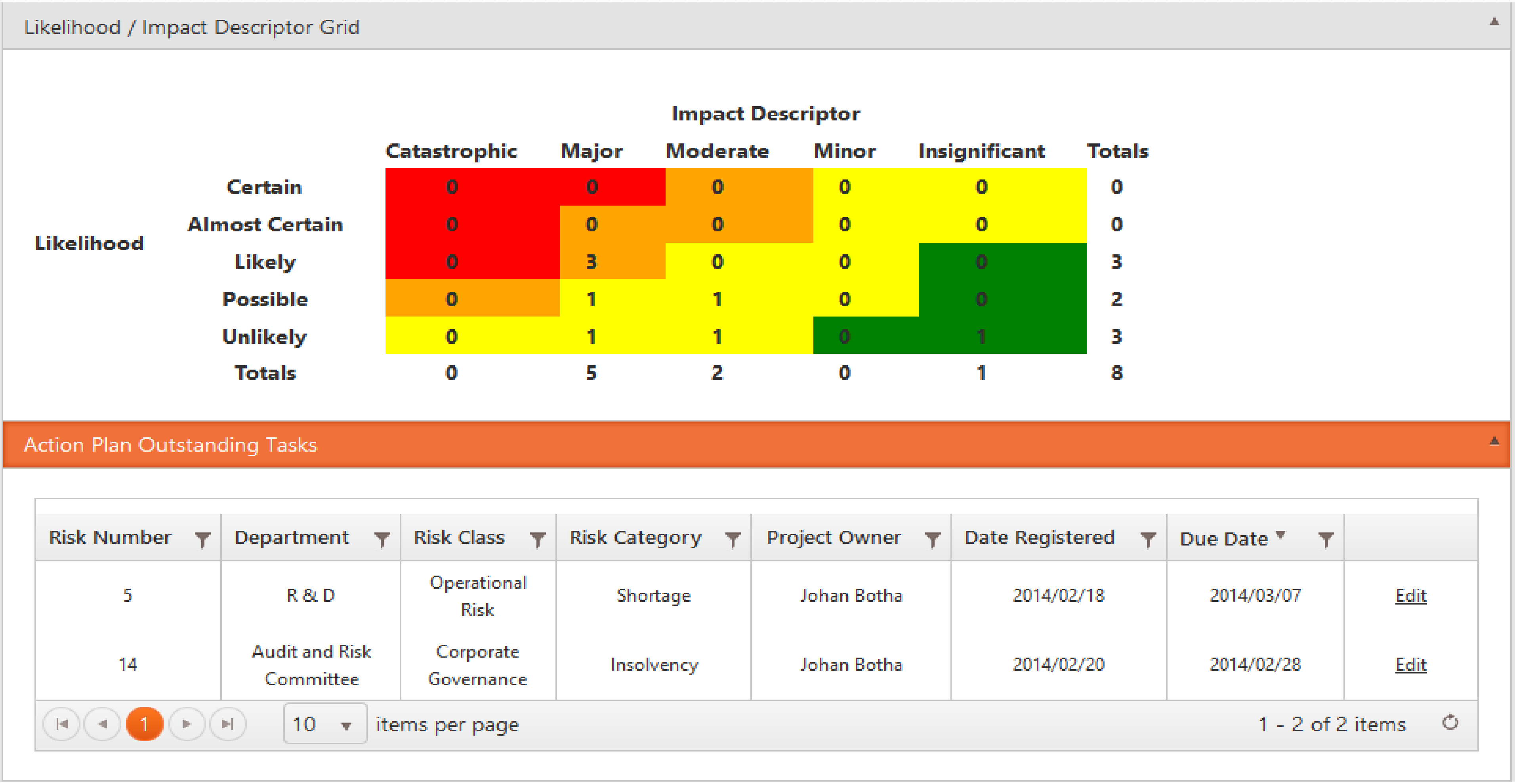
Cyber Risk Assessment Example

Information Asset	Value High/ Low/ medium	Risk High/ Low/ medium	Recovery Mitigation Cost	Priority	Options
Board Minutes	High	Low	Low	Medium	Accept: no new control Transfer: store with a vendor offsite Limit: save to microfilm, purchase fireproof cabinet Avoid: N/A
Personnel Records	High	High (Identity Theft)	High	High	Accept: no new controls Transfer: store with a vendor offsite Limit: encrypt information Avoid: disconnect computer from the Internet

CREATE YOUR FIRM’S CYBER RISK UNIVERSE

- Human Risk
- Governance Risk
- Malware Risk
- Fraud Risk
- Reputation Risk
- Vendor Risk
- Flaws & Bugs
- Escalation Risk
- Regulatory Risk
- Outsourcing Risk
- Technology Risk
- Vulnerabilities
- Project Risk
- Encryption Risk
- Disruption Risk
- Compliance Risk
- Monitoring Risk
- Legal Risk
- Audit
- Application Risk
- Threats Risk
- Reporting Risk
- PCI DSS

OPERATIONAL RISK MANAGEMENT
RISK HEAT MAP



Likelihood / Impact Descriptor Grid

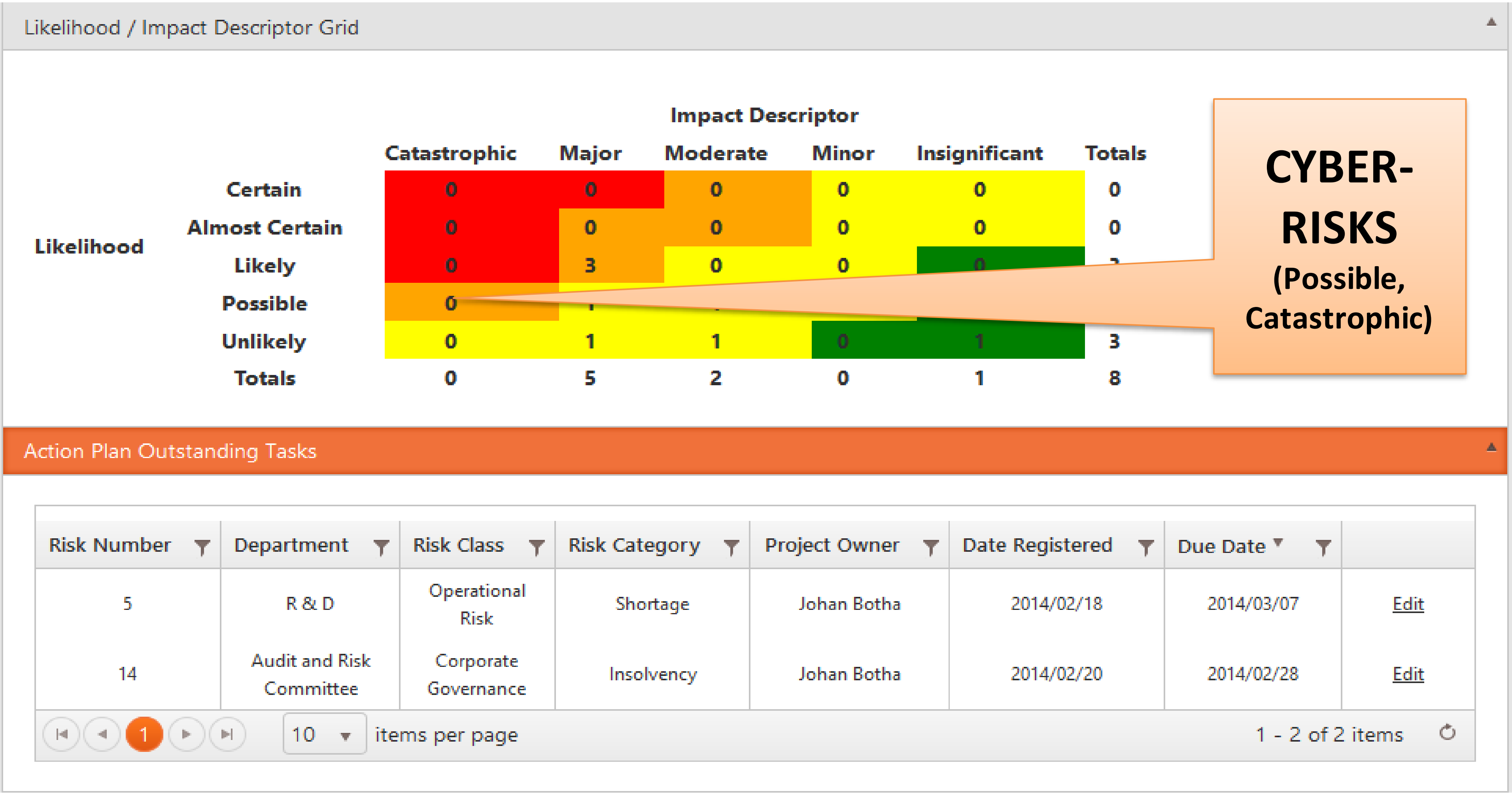
Impact Descriptor

Likelihood		Catastrophic	Major	Moderate	Minor	Insignificant	Totals
	Certain	0	0	0	0	0	0
	Almost Certain	0	0	0	0	0	0
	Likely	0	3	0	0	0	3
	Possible	0	1	1	0	0	2
	Unlikely	0	1	1	0	1	3
	Totals	0	5	2	0	1	8

Action Plan Outstanding Tasks

Risk Number	Department	Risk Class	Risk Category	Project Owner	Date Registered	Due Date	
5	R & D	Operational Risk	Shortage	Johan Botha	2014/02/18	2014/03/07	Edit
14	Audit and Risk Committee	Corporate Governance	Insolvency	Johan Botha	2014/02/20	2014/02/28	Edit

OPERATIONAL RISK MANAGEMENT
RISK HEAT MAP



Likelihood / Impact Descriptor Grid

Impact Descriptor

		Catastrophic	Major	Moderate	Minor	Insignificant	Totals
Likelihood	Certain	0	0	0	0	0	0
	Almost Certain	0	0	0	0	0	0
	Likely	0	3	0	0	0	[illegible]
	Possible	0	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
	Unlikely	0	1	1	0	1	3
	Totals	0	5	2	0	1	8

CYBER-RISKS
(Possible, Catastrophic)

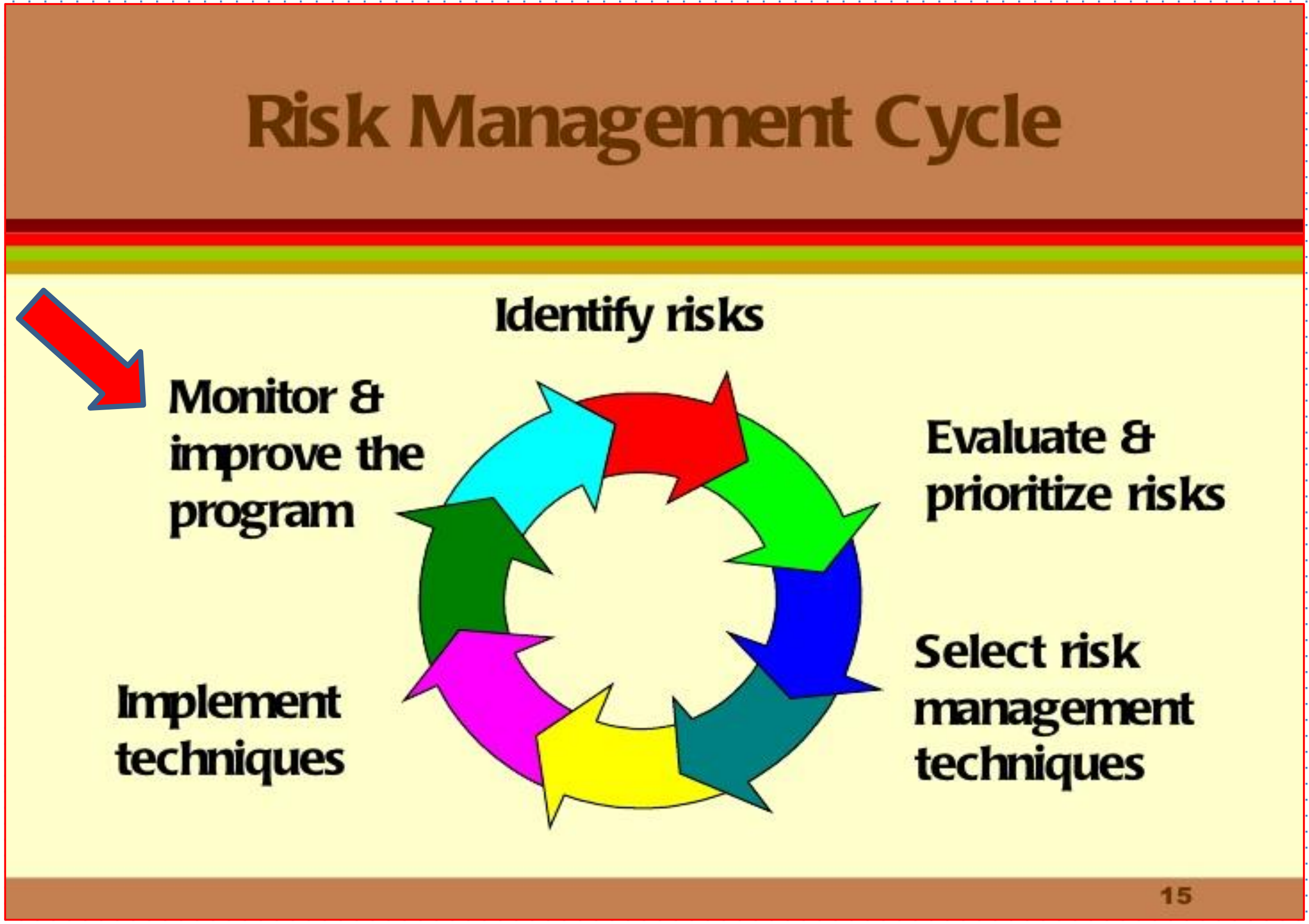
Action Plan Outstanding Tasks

Risk Number	Department	Risk Class	Risk Category	Project Owner	Date Registered	Due Date	
5	R & D	Operational Risk	Shortage	Johan Botha	2014/02/18	2014/03/07	Edit
14	Audit and Risk Committee	Corporate Governance	Insolvency	Johan Botha	2014/02/20	2014/02/28	Edit

1 · 10 items per page · 1 - 2 of 2 items

OPERATIONAL RISK MANAGEMENT
RISK HEAT MAP

Strong Risk Culture



Risk Management Cycle

Identify risks

Evaluate & prioritize risks

Select risk management techniques

Implement techniques

Monitor & improve the program

15

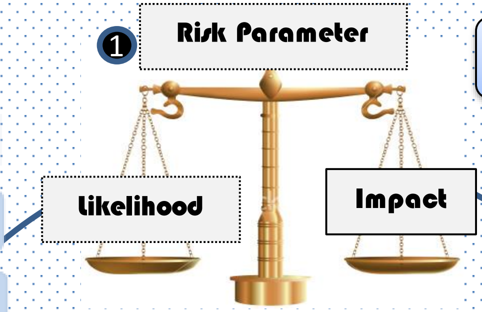
Cyber Risk Governance

MONITOR & IMPROVE OPS RISK PROGRAM

Define Key Risk Indicators

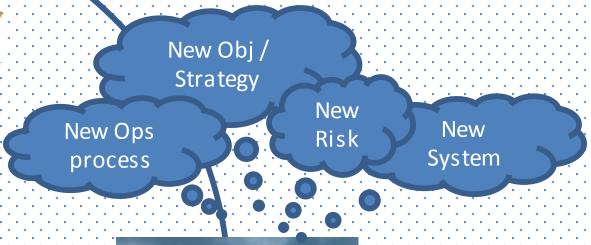
- Risk Scores
- Time Frame
- Risk Escalation

1

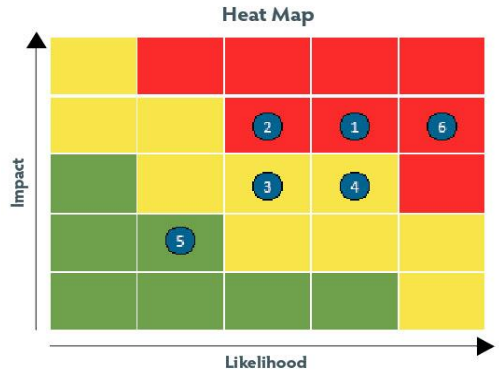


Risk Score = Likelihood x Impact

2



4



3

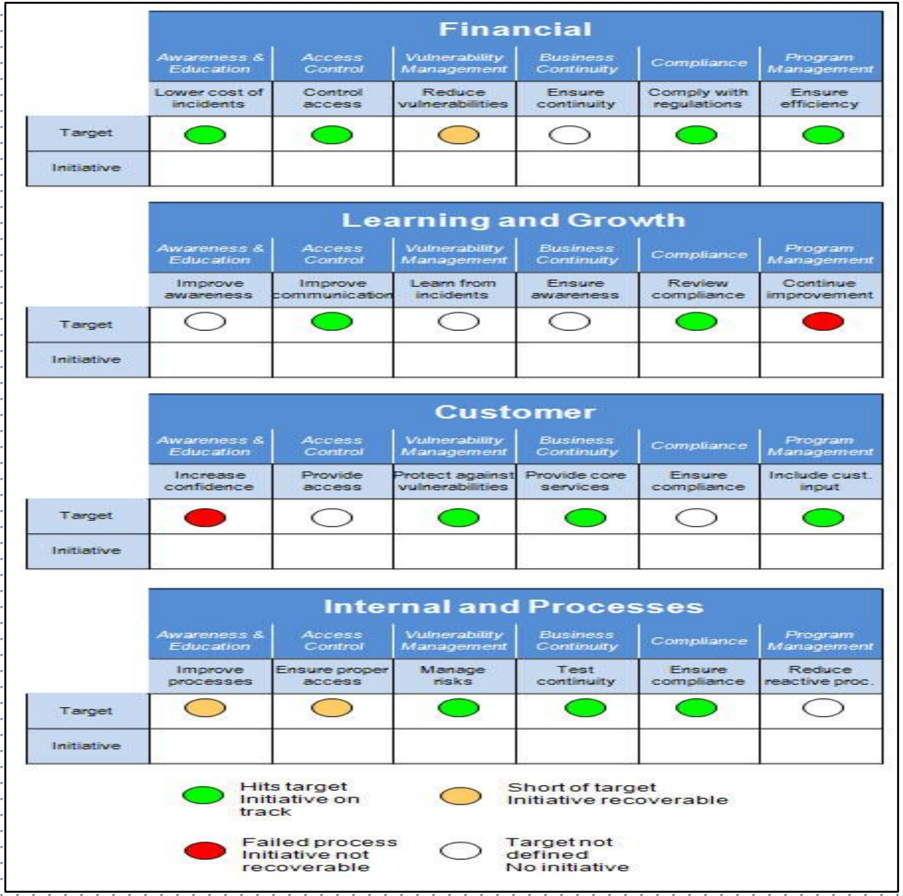
Tier 1 Tier 2 Tier 3

Economic	1	2	3	4	5
Operational	1	2	3	4	5
Brand & Reputation	1	2	3	4	5
Regulatory	1	2	3	4	5
Client	1	2	3	4	5
Impact	Insignificant	Minor	Moderate	Major	Severe

How can Key Risk Indicators (KRIs) effectively interact with other tools to monitor attempts of cyber-attacks?

KRI Metrics	Risk Owners	Scope of Responsibilities
Percentage of Failure rates	Technology Team	Product and/or services Failure Testing Cycles
Volume of data passing thru' network traffic	Security & Risk Team	Managing data traffic passing thru' firewalls' defenses via setting up filter rules for data packets.
System disruptions	Business, Technology, Security & Risk	Managing system downtime, investigate root causes & incident escalation

How can Key Risk Indicators (KRIs) effectively interact with other tools to monitor attempts of cyber-attacks?



	Financial					
	Awareness & Education	*Access Control*	*Vulnerability Management*	*Business Continuity*	*Compliance*	*Program Management*
	Lower cost of incidents	Control access	Reduce vulnerabilities	Ensure continuity	Comply with regulations	Ensure efficiency
Target	🟢	🟢	🟠	○	🟢	🟢
Initiative						

	Learning and Growth					
	Awareness & Education	*Access Control*	*Vulnerability Management*	*Business Continuity*	*Compliance*	*Program Management*
	Improve awareness	Improve communication	Learn from incidents	Ensure awareness	Review compliance	Continue improvement
Target	○	🟢	○	○	🟢	🔴
Initiative						

	Customer					
	Awareness & Education	*Access Control*	*Vulnerability Management*	*Business Continuity*	*Compliance*	*Program Management*
	Increase confidence	Provide access	Protect against vulnerabilities	Provide core services	Ensure compliance	Include cust. input
Target	🔴	○	🟢	🟢	○	🟢
Initiative						

	Internal and Processes					
	Awareness & Education	*Access Control*	*Vulnerability Management*	*Business Continuity*	*Compliance*	*Program Management*
	Improve processes	Ensure proper access	Manage risks	Test continuity	Ensure compliance	Reduce reactive proc.
Target	🟠	🟠	🟢	🟢	🟢	○
Initiative						

🟢 Hits target Initiative on track

🟠 Short of target Initiative recoverable

🔴 Failed process Initiative not recoverable

○ Target not defined No initiative

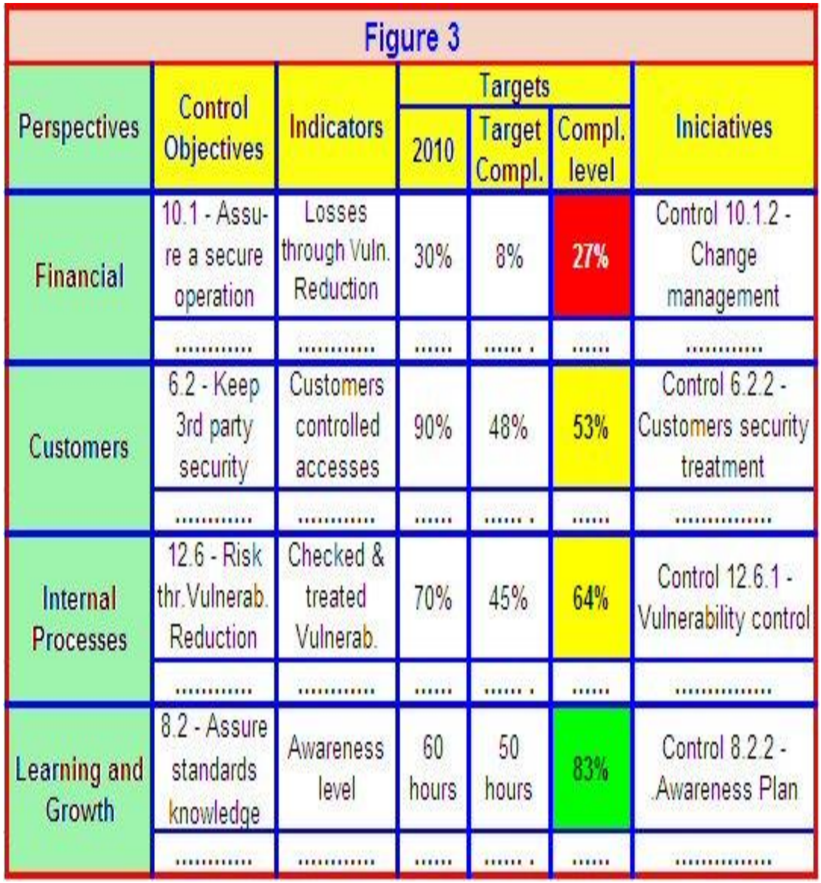


Figure 3

Perspectives	Control Objectives	Indicators	Targets			Iniciatives
			2010	Target Compl.	Compl. level	
Financial	10.1 - Assu-re a secure operation	Losses through Vuln. Reduction	30%	8%	27%	Control 10.1.2 - Change management
	....	....	......	....	......	....
Customers	6.2 - Keep 3rd party security	Customers controlled accesses	90%	48%	53%	Control 6.2.2 - Customers security treatment
	....	....	......	....	......	....
Internal Processes	12.6 - Risk thr. Vulnerab. Reduction	Checked & treated Vulnerab.	70%	45%	64%	Control 12.6.1 - Vulnerability control
	....	....	......	....	......	....
Learning and Growth	8.2 - Assure standards knowledge	Awareness level	60 hours	50 hours	83%	Control 8.2.2 - Awareness Plan
	....	....	......	....	......	....

Interplay of Incident Response and Business Continuity planning.

CURRENT STATE OF CYBER INCIDENT RESPONSE

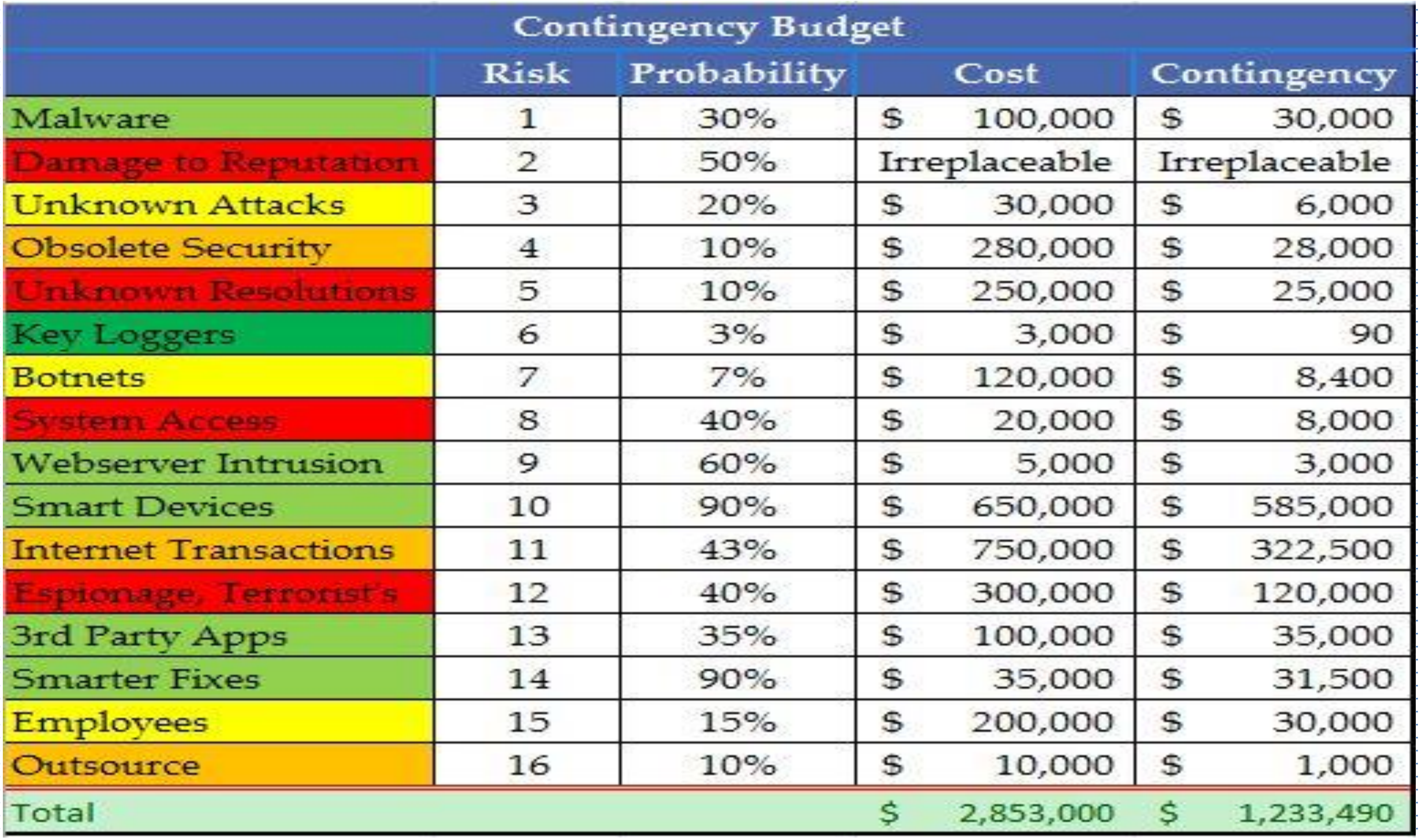
CYBER-ATTACKS CAN STRIKE WITHIN SECONDS!

DATA CAN BE STOLEN WITHIN MINUTES!

Interplay of Incident Response and Business Continuity planning. (NETS & CCB)

LOW CYBER INCIDENTS			HIGH CYBER INCIDENTS		
Notification	Timing	Ownership	Notification	Timing	Ownership
Biz Unit Dept Head	Immediate	Biz Unit Dept Head	Senior Mgmt	Immediate	CEO
ORM Dept Head	< 30 mins	-	ERM + ORM Dept Heads	Immediate	-
Cyber Alert Team	< 45 mins	-	Cyber Alert Team	Immediate	

Interplay of Incident Response and Business Continuity planning(NETS & CCB) .



Contingency Budget

	Risk	Probability	Cost	Contingency
Malware	1	30%	$ 100,000	$ 30,000
Damage to Reputation	2	50%	Irreplaceable	Irreplaceable
Unknown Attacks	3	20%	$ 30,000	$ 6,000
Obsolete Security	4	10%	$ 280,000	$ 28,000
Unknown Resolutions	5	10%	$ 250,000	$ 25,000
Key Loggers	6	3%	$ 3,000	$ 90
Botnets	7	7%	$ 120,000	$ 8,400
System Access	8	40%	$ 20,000	$ 8,000
Webserver Intrusion	9	60%	$ 5,000	$ 3,000
Smart Devices	10	90%	$ 650,000	$ 585,000
Internet Transactions	11	43%	$ 750,000	$ 322,500
Espionage, Terrorist's	12	40%	$ 300,000	$ 120,000
3rd Party Apps	13	35%	$ 100,000	$ 35,000
Smarter Fixes	14	90%	$ 35,000	$ 31,500
Employees	15	15%	$ 200,000	$ 30,000
Outsource	16	10%	$ 10,000	$ 1,000
Total			$ 2,853,000	$ 1,233,490

KEY TAKEAWAYS

Part 1 - Cyber Security Threats

- Aware of high risk/profile threats + their rising sophistication/ scale.
- Huge Gaps in Cyber Defense Technologies and Expertise.
- Ideas to use big data, analytics & intelligence to combat threats.
- Common goals in collaborating with peers and regulators.

Part 2 - Defending against Cyber Threats/ORM Perspective

- Need to set-up cyber risk governance.
- Know how to identify & protect key assets against cyber threats.
- Define key KRIs metrics to monitor attempts of cyber-attacks.
- Understanding the problem in Incident Response and to use Business Continuity planning to address them.

Some Useful References:

- Andrew Koh : “Rethinking enterprise risk management – A new educational series looking at practical ideas for managing a variety of risks”, (StrategicRISK, Asia edition, Issue 5, Sep. 2014): file:///C:/Users/Andrew%20Koh/Downloads/SR-Asia-September-2014.pdf
- Andrew Koh : “Rethinking enterprise risk management – Our Educational Series Examines Emerging Risks and Scenario Analysis (StrategicRISK, Asia edition, Issue 6, Jan 2015): http://edition.pagesuite-professional.co.uk//launch.aspx?eid=75224692-730f-4804-998c-cfad87fbc0b2
- Models of Escalation and De-escalation in Cyber Conflict John C. Mallery Computer Science & Artificial Intelligence Laboratory Massachusetts Institute of Technology Presentation at the 2011 Workshop on Cyber Security and Global Affairs, Budapest, Hungary, May 31 – June 2, 2011.Version: 3/29/2012 11:04 AM
- Verizon 2015 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2015/
- An ISACA and RSA Conference Survey: State of Cybersecurity: Implications for 2015: http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2015.aspx
- CISCO Annual Security Report 2015: http://www.cisco.com/web/offers/lp/2015-annual-security-report/index.html

If You Have Trouble Sleeping After This….

Contact Information

YAHOO! Mail andrewkohmw@yahoo.com.sg

LinkedIn https://sg.linkedin.com/in/andrewkohmw

twitter @KohWee

NYU Leonard N. Stern School of Business
Master of Science Risk Management
RISK MANAGEMENT
SYMPOSIUM 2015

“Defending Against Cyber Security Threats to the Payment and Banking Systems”

Andrew Koh
Class of 2010 MSRM
Class of 2009 MSGF

Q & A