CFO Breakfast Talk

Cyber Risk, Data Protection & Analytics

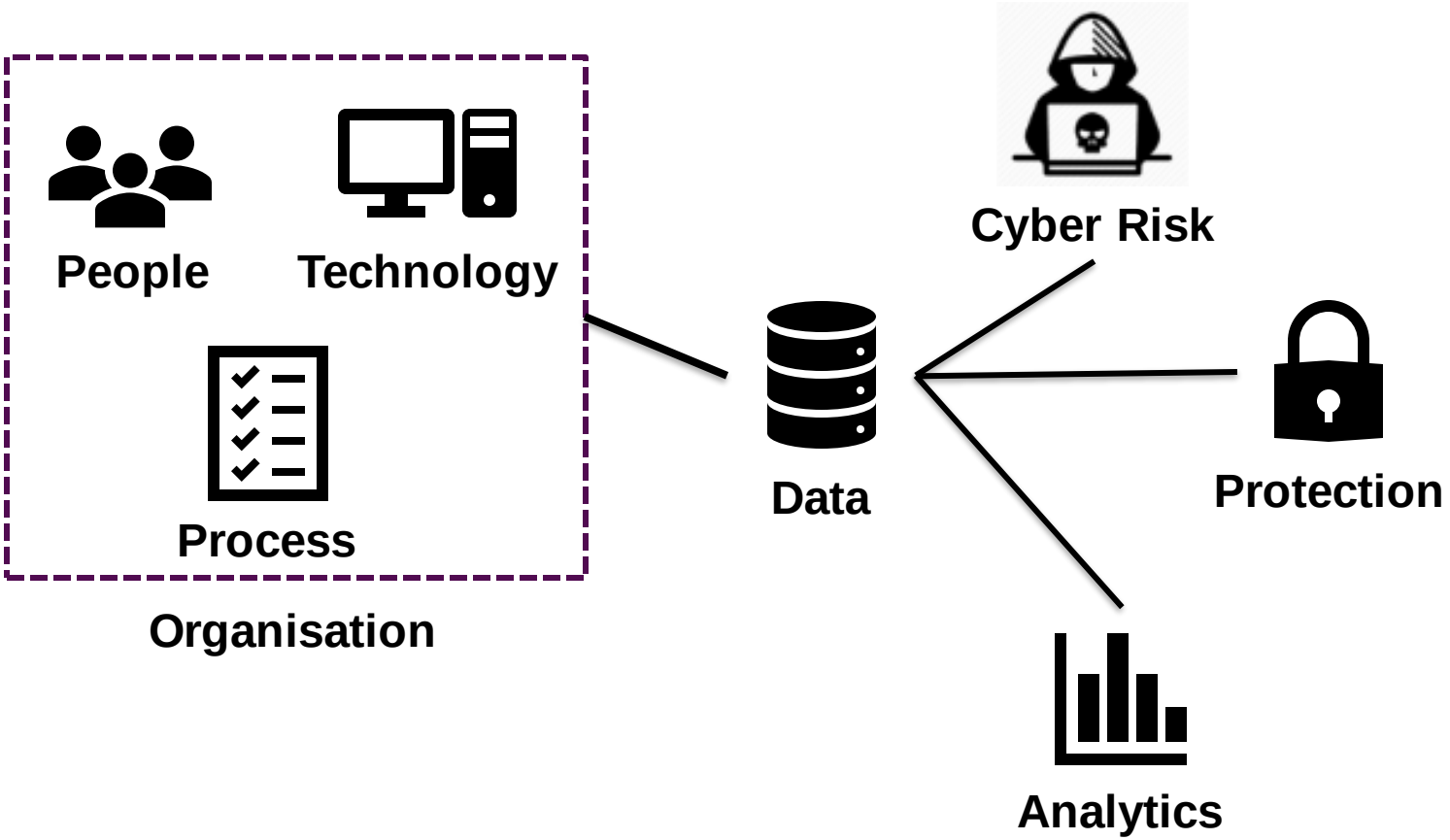
24 August 2018

Alvin Soh

Background: 15 years of working experience in providing IT Assurance and Advisory Services

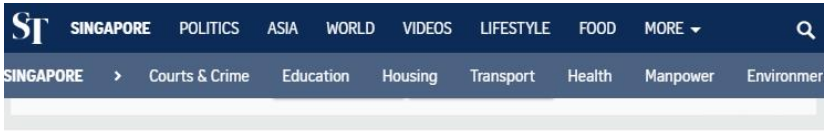
Role: Senior Manager, Moore Stephens Risk Management

Overview


People
Technology
Process
Organisation
Data
Cyber Risk
Protection
Analytics


COMPUTER
DESIGN
PROTECTION
DEFECTS
CYBER
SYSTEM
DEFENSE
POWER
LEVEL
WELL
LOSS
INTERNATIONAL
PROTECTING
COMPROMISED
HOUSE
INFORMATION
BASED
USED
STATES
NEW
SITE
COMPUTERS
BILL
PROTECT
INCLUDE
SERVICES
PRIMARY
SECURE
INTRUSION
TECHNOLOGY
OPERATING
NATIONAL
FLAWS
MANAGEMENT
INTERNET
ORDER
PROVIDE
ASSURANCE
MAIN
INFRASTRUCTURE
SECURITY
SYSTEMS
MANY
ACT
DATA
AIR
ISSUES
LEVELS
PROBLEM
ENSURE
CODE
HIGH
USING
NETWORK
UNITED
ACCESS
WORLD
LEGAL
CENTER
IMPLEMENTED
SEGMENTS
CODING
TECHNIQUES
NEEDED
SOFTWARE
HARDWARE
USE
COMMUNICATIONS
APPLICATION
CAPABILITIES
ATTACK
COMMON
NETWORKS
DESIGNED
KNOWN
CRITICAL
CYBERCRIME
CONNECTED
POLICY
GOVERNMENT
ONE
CYBERSECURITY
FILES
ENGINEERING
ARTICLE
CONTROL
ANOTHER
VULNERABILITIES

Data Breaches



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack

- The healthcare industry has been a victim of cyber attacks because of the value of healthcare data - such as medical histories - which can be used for a variety of cyber fraud.
- Healthcare institutions are vulnerable partly because healthcare operators are adopting electronic health records and other advances even if they weren't ready to adequately invest in security.

Data Breaches

MAS orders financial institutions to tighten customer verification after SingHealth data breach

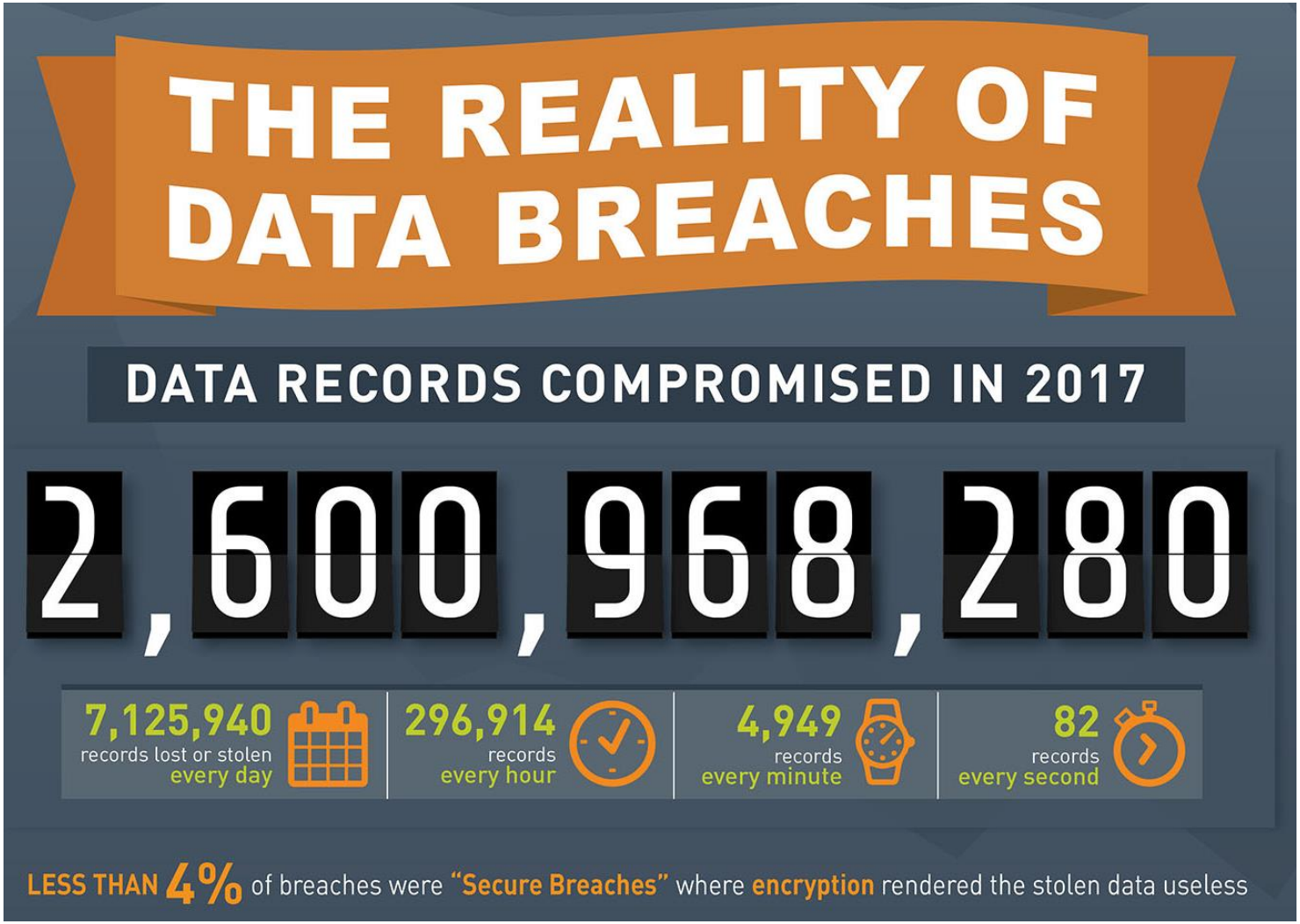
Staff Writer, Singapore
Yahoo News Singapore 24 July 2018

(Reuters file photo)

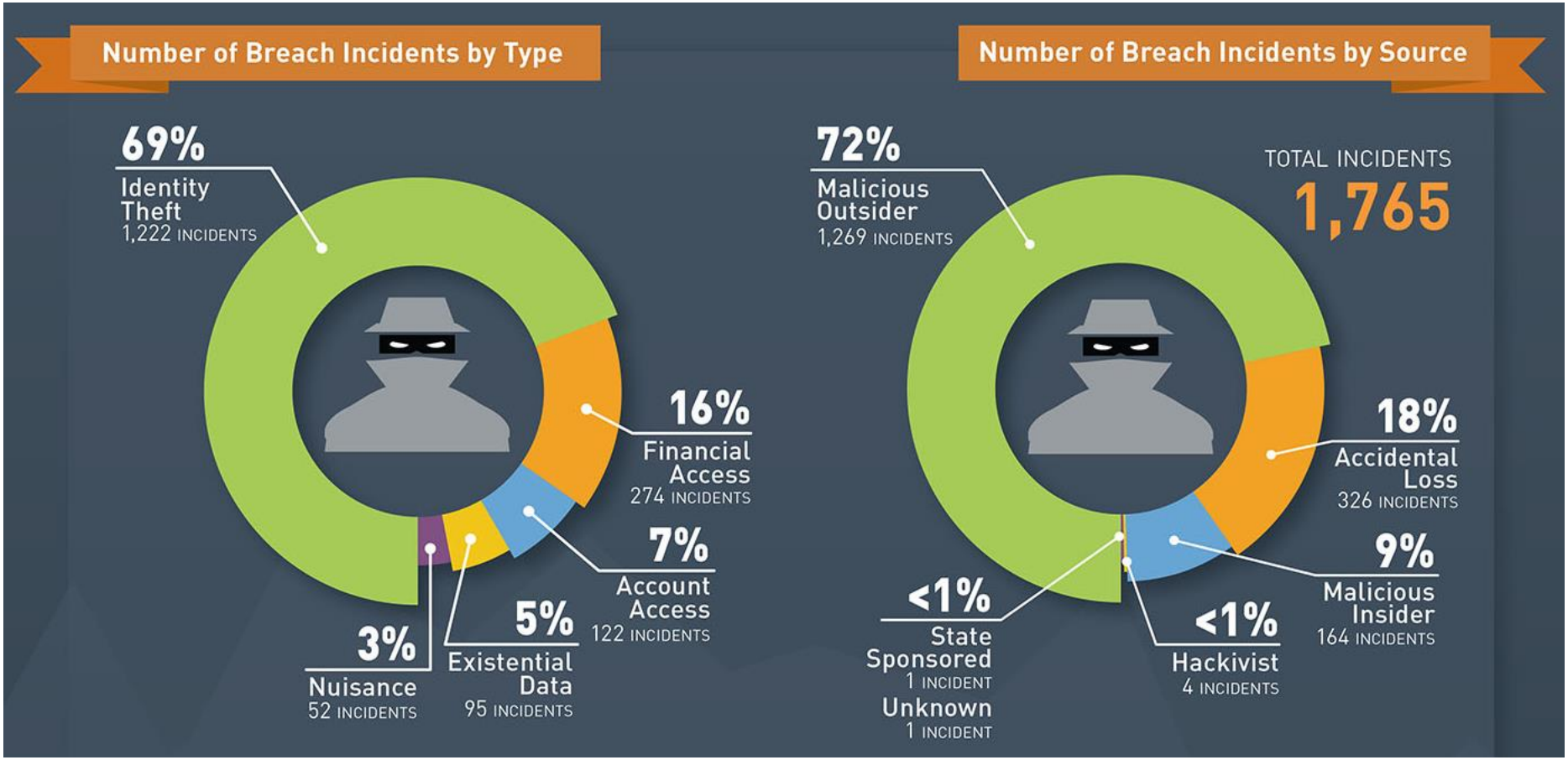
Impact of stolen personal data

- Personal info that was stolen are often used as the first level of basic customer verification.

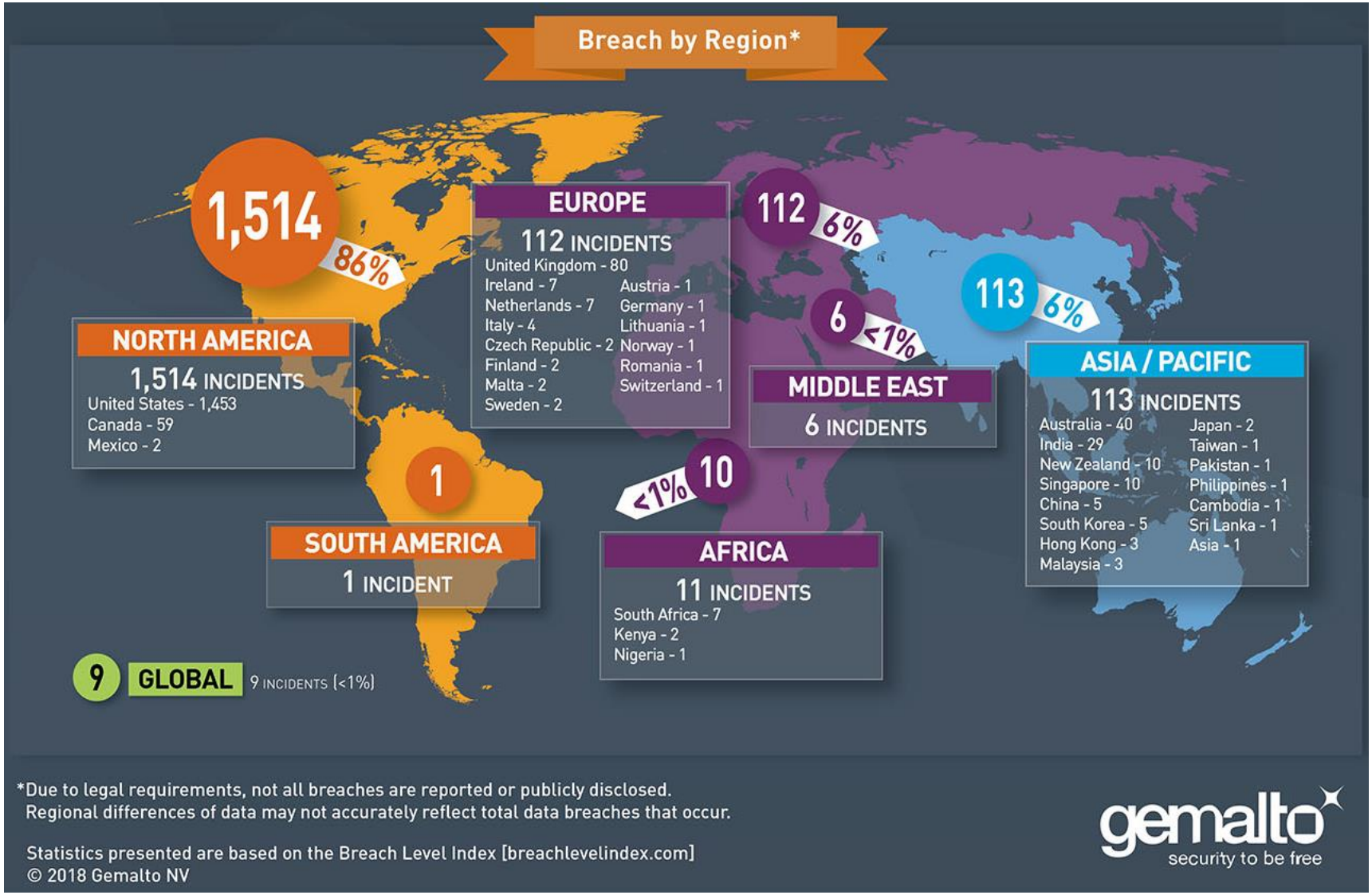
Data Breaches



Data Breaches



Data Breaches

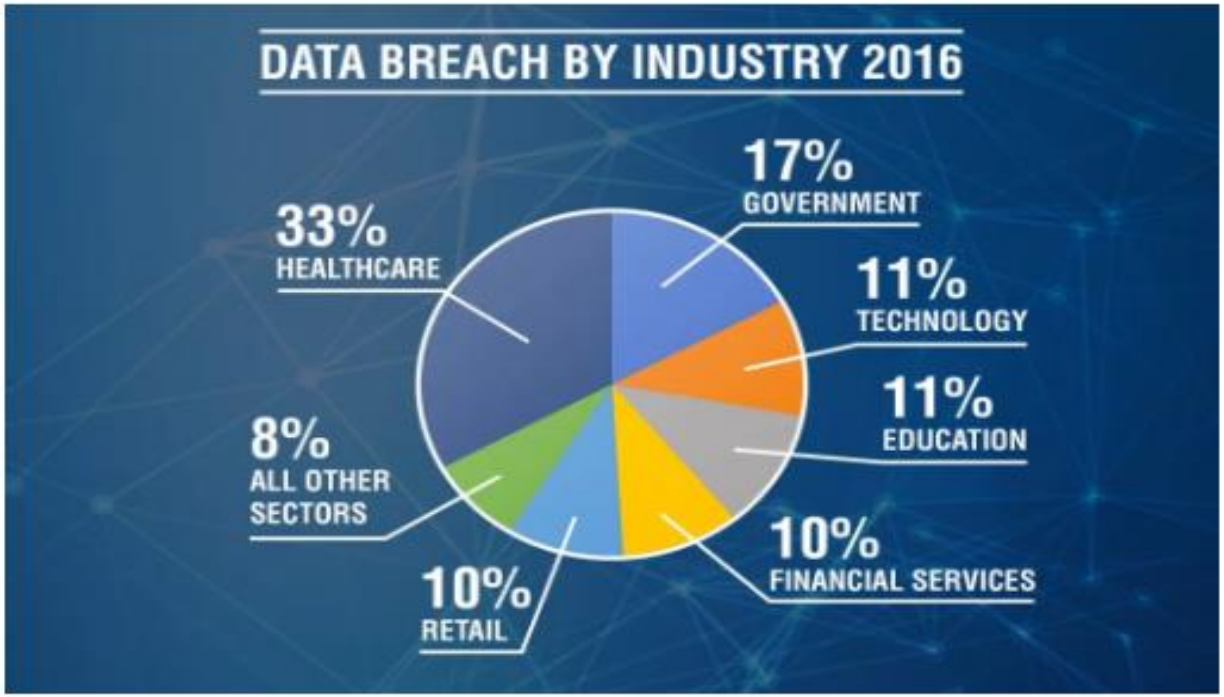


*Due to legal requirements, not all breaches are reported or publicly disclosed.
Regional differences of data may not accurately reflect total data breaches that occur.

Statistics presented are based on the Breach Level Index [breachlevelindex.com]

gemalto
security to be free

Data Breaches



Data from 2016 Financial Industry Cyber Security Report. Security ScoreCard.

https://cdn2.hubspot.net/hubfs/533449/SecurityScorecard_2016_Financial_Report.pdf

- A study done by IT consultant CGI and Oxford Economics concluded that severe breaches caused share prices to fall an average of 1.8% on a permanent basis.

Who are we protecting against

Insiders

Nation States

Hacktivists

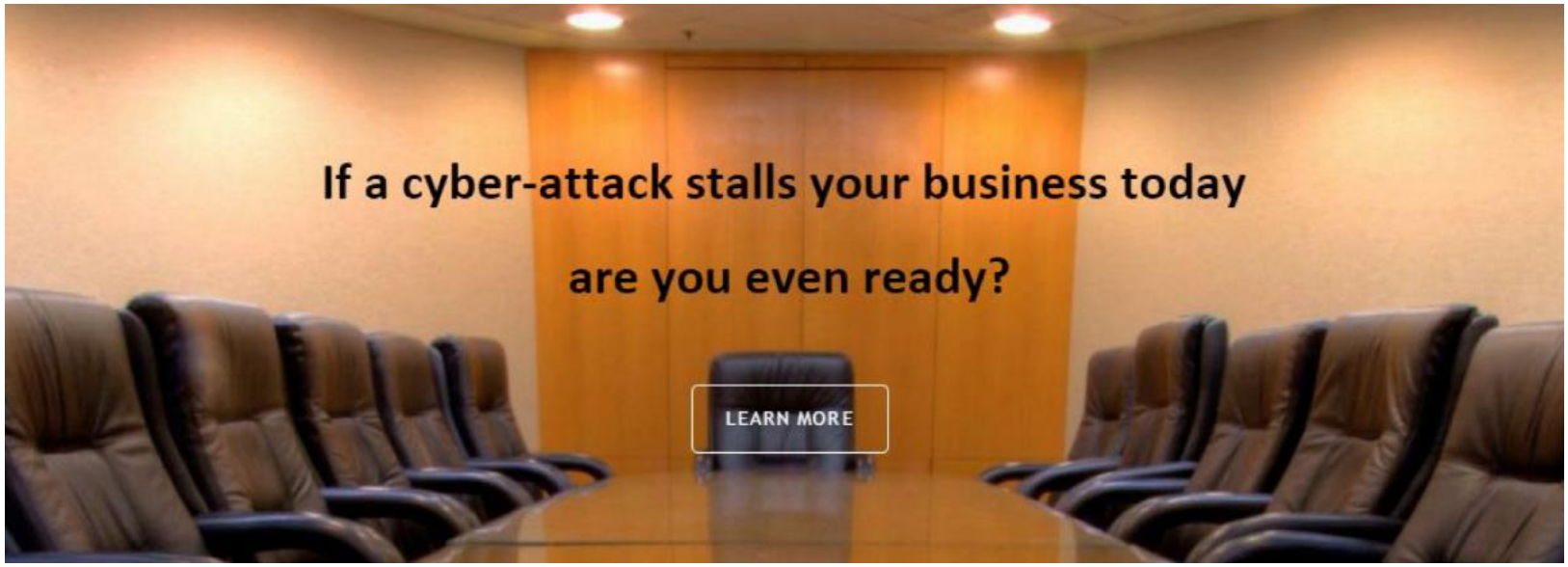
Cyber Terrorists

Organized Crimes

Business Impact and Risk

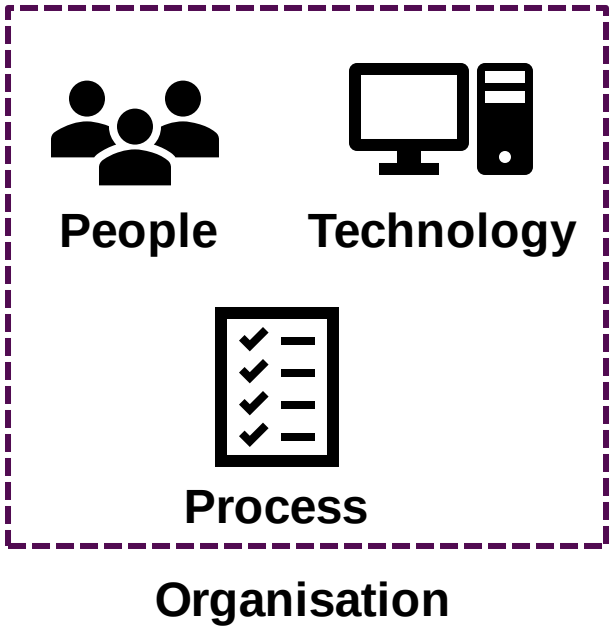
- Negative publicity resulting in loss of reputation
- Fines, lawsuits and legal fees resulting from non-compliance or loss of confidential or consumer information
- Forensic investigation costs
- Public relations campaign costs to improve public image
- Loss of intellectual property or trade secrets
- Technology improvement costs to mitigate and improve cybersecurity controls
- Loss of time and productivity

Think About It…



Cyber security risks should be given priority and not as an after thought or only after occurrence of a cyber-incident.

Are you ready?



- Business usually focus on technology to manage cyber risk.
- When it comes to cybersecurity, the people and process matter as much as technology, if not more.

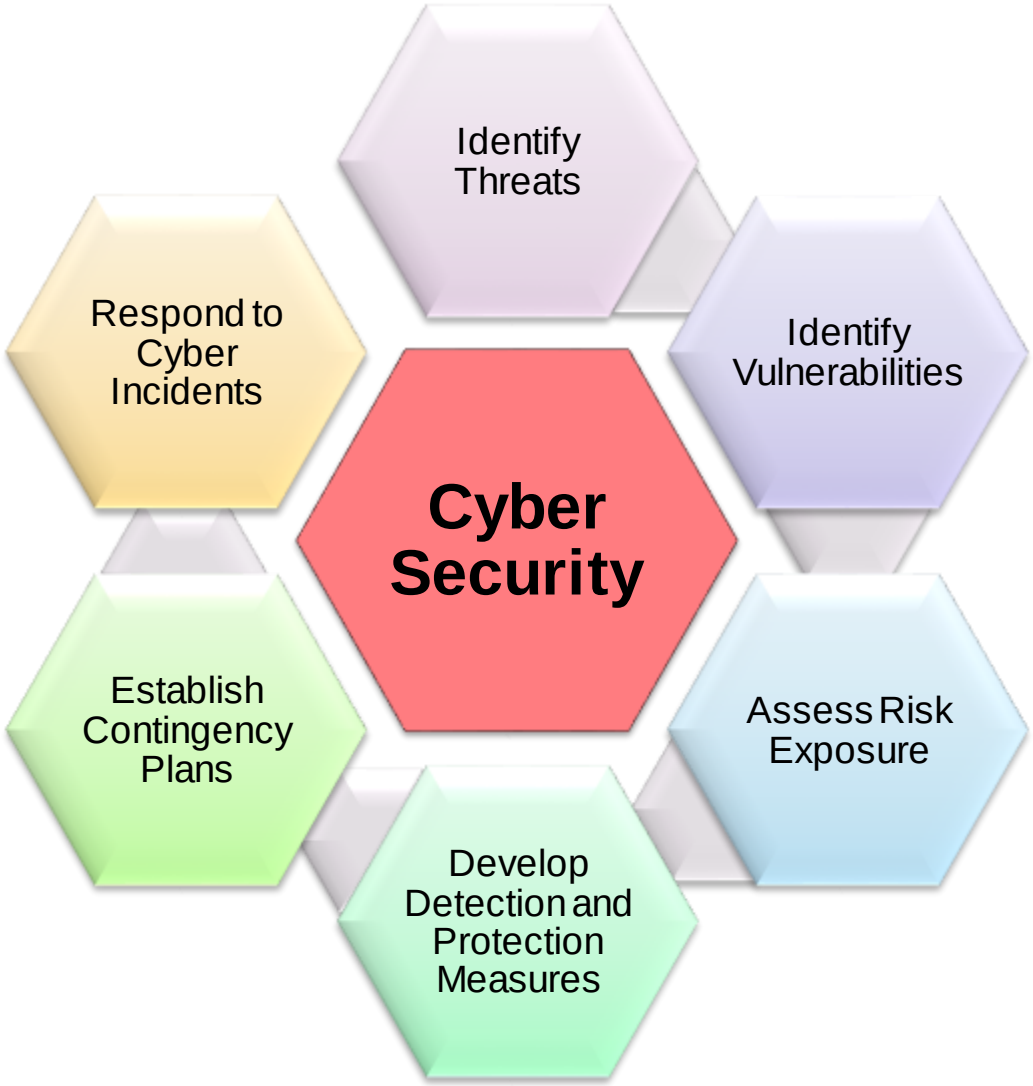
Reducing Cyber Risks

People	Process	Technology
Briefing to new staff on IT security requirement	Review and update IT security policies e.g. password management	Control the use of personal smart devices and USB storage devices
Conduct IT security awareness training for staff & vendors	Establish data recovery procedures & equipment disposal policy	Secure configuration for hardware and software and up-to-date patches
Quarterly emails/circular on new cyber threats	Establish and test cyber incident response framework	Implement appropriate network security measures e.g. anti-virus, firewalls, IDS & IPS
Report breaches and phishing attempts	Conduct periodic user access review and monitor the use of admin administrator privileges	Secure physical parameters to server room

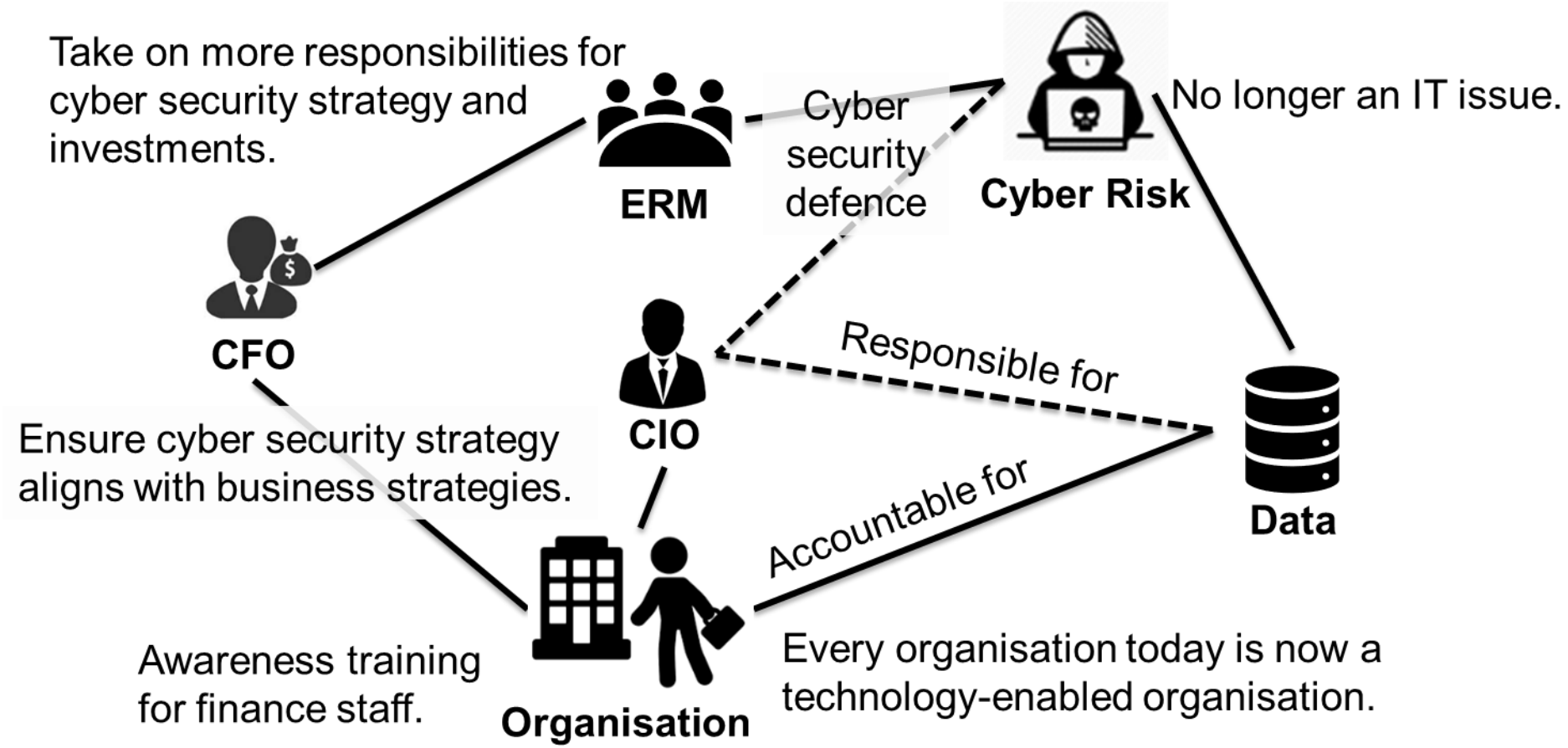
NIST Cyber Security Framework

NIST - National Institute of Standards and Technology (NIST)

Simplified Approach to Cyber Security



Changing Role of CFO



Next Steps?


Cybersecurity
Intrusion Tests
Vulnerability
Investigation
Cyber Defenses
Corrective Actions
Audits


DATA
PROTECTION
INFORMATION
PERSONAL
INTERNET
PARTIES
MEDICAL
ANONYMIZERS
ACTIVITIES
CONCERN
NETS
PRIVACY
CASES
ENCRYPTED
E-MAILS
ACCESS
PERSON
REVEAL
THIRD
MIX
WISH
BECOME
CONNECTION
SITES
ORDER
INDIVIDUALS
WELL
FAIR
ABILITY
TRACK
CALLED
ONLINE
BROWSING
FINANCIAL
PURCHASES
PATIENTS
CONTROL
INCLUDE
DONE
REQUIRED
VISITED
WEBPAGES
SOURCE
TRUSTED
READ
KNOW
ALSO
PHYSICIAN-PATIENT
ONESELF
OTHERS
REVEALS
TRACELESS
DISTRIBUTED
AWAY
AUDIENCE
MIGHT
USE
WITHOUT
SOMEONE
GIVE
USED
MUCH
TRAFFIC
PRACTICES
WEB
THIRD
STREAM
SOMETHING
PRIVILEGE
BROADCASTING
MAINTAINING
OPEN
AMOUNT
ONE
ONE'S
WHETHER
ADDITION
HEALTH
RECORDS
CREATED
RATING
STATES
PERFORMED
COMBINED
CONFIDENTIALITY
REPRESENT
FTC
DIGNITY

Data Protection

- Data protection is the process of safeguarding important information from corruption, compromise or loss.

- Data privacy refers to the act of protecting the integrity, confidentiality, and availability of personal information that are collected, stored, and processed.

Data Protection

ST SINGAPORE POLITICS ASIA WORLD VIDEOS LIFESTYLE FOOD MORE

SINGAPORE › Courts & Crime Education Housing Transport Health Manpower Environmer

Singapore's privacy watchdog to investigate SingHealth data breach

The SingHealth attack, which was made known to the public on July 20, compromised the personal particulars of about 1.5 million patients, including those of Prime Minister Lee Hsien Loong. ST PHOTO: ARIFFIN JAMAR

Personal data was stolen from the data breach.

Data Protection Regulations

European Union General Data Protection Regulation (GDPR)

The EU GDPR entered into force on 25 May 2018 as the primary law regulating how companies protect EU citizens' personal data.

Under the GDPR, personal data can include a name, a photo, an e-mail address, bank details, posts on social media websites, medical information, or a computer IP address.

GDPR – Key requirements

Increased Territorial Scope

- Applies to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Penalties

- For serious breach infringements of the regulation, can be fined **up to 4% of global turnover or €20 million – whichever is greater**.

Consent

- Conditions surrounding consent have been strengthened. Must be given in intelligible and easily accessible form using clear and plain language.
- Silence, pre-ticked boxes and inactivity will no longer suffice as consent.
- Organisations must be able to evidence consent.
- Consent can be withdrawn at any time.

GDPR – Key requirements

Breach Notification

- Data breaches must be reported to the data protection authority within 72 hours of discovery and individuals impacted should be told where there exists a high risk to their rights and freedom.

Data portability

- Data subjects now have the right to receive the personal data concerning them in a commonly used and machine readable format that can be transferred to another data controller.

Right to access

- Data subjects now have a right to obtain from the data controller confirmation that personal data concerning them is being processed, where and for what purpose.

GDPR – Key requirements

Right to be correct

- Data subjects now have the right to correct inaccurate personal data.

Right to be forgotten

- Data subjects now have the right to be forgotten.

Privacy by design

- Legal requirement within GDPR, which calls for the inclusion of data protection from the onset of the designing of systems rather than an addition. This includes conducting data protection impact assessments (DPIAs) for high-risk processing operations.

Data protection officer (DPO)

- Inform and advise the organisation of its obligations, monitor compliance, including awareness raising, staff training and audits. DPO also cooperate with data protection authorities and act as a contact point.

GDPR – Data protection principles

Personal data must be processed according to the six data protection principles:

- Processed lawfully, fairly and transparently.
- Collected only for specific legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Must be accurate and kept up to date.
- Stored only as long as is necessary.
- Ensure appropriate security, integrity and confidentiality.

Data Protection Framework – Approach

Identify Business Data Owners	Establish a list of IT applications and assign appropriate data owners.
Classify Data	Define sensitive data elements such as customer and employee personal data and assign classification based on **C**onfidentiality, **I**ntegrity, **A**vailability and **C**onsent.
Assign Compliance Controls	Assign appropriate controls such as DLP, data encryption, data masking and etc based on the data classification (e.g. public, internal, confidential).
Compliance Monitoring	Monitor for non-compliance such as data retention period, data leakage and tracking of data breaches.
Management Reporting	Provide updates to the board of the monitoring results of compliance gaps, data leaks and new risks.

Cyber Risk and Data Protection

Tips to achieve GDPR compliance and protect data against cyber threats

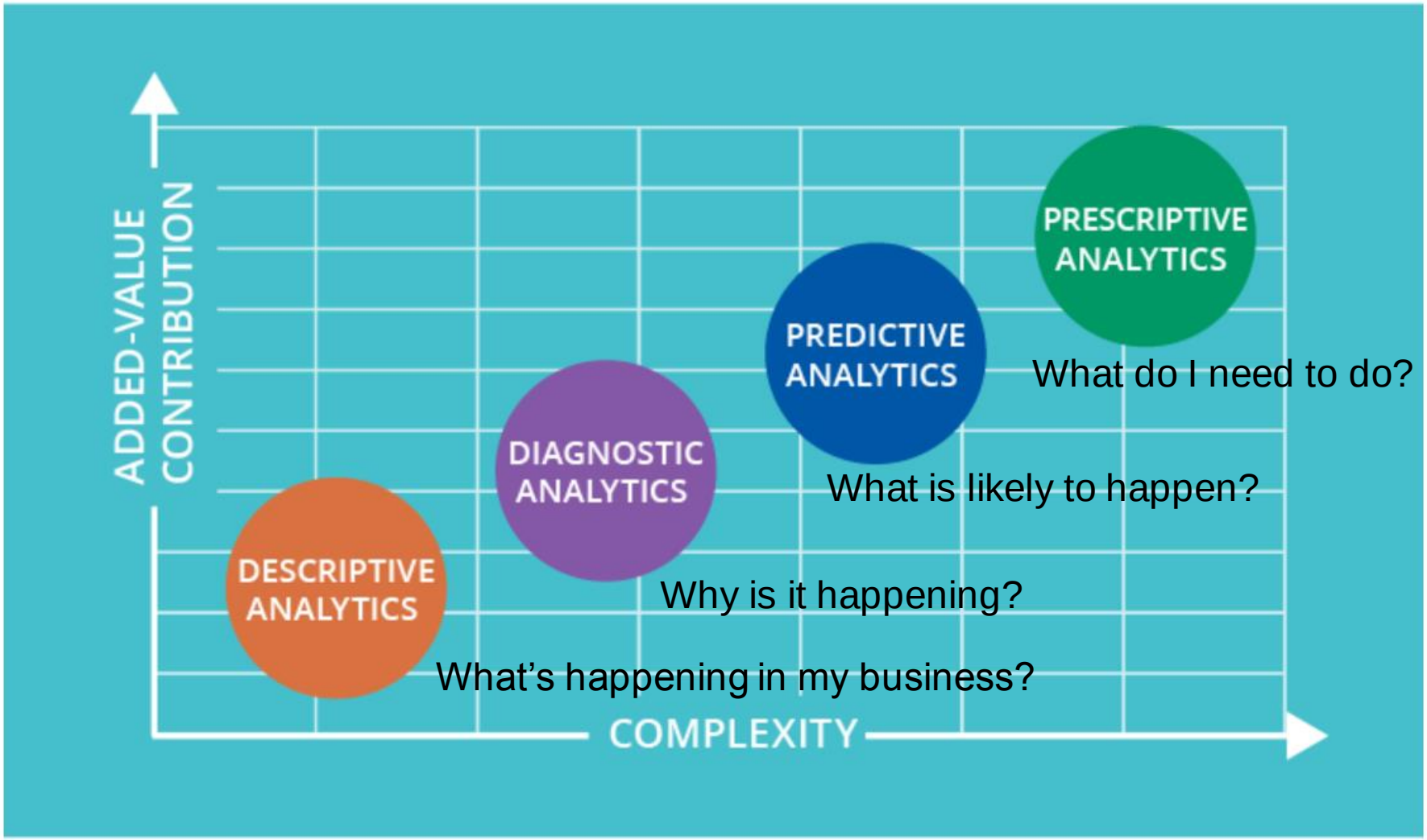
- Know what data you have and where it is
- Protect your IT systems and data and have the ability to render data unusable
- Employees need to be aware of privacy risks and how data should be handled. Likewise, business processes need to be designed with privacy in mind.
- Continuously monitor your current business to establish if the technologies you have in place are appropriate as IT systems, security threats and company practices change.
- Regularly test your data breach plan.

Next Steps

People	Process	Technology
Appoint a Data Protection Officer (where necessary)	Review practices and process to ensure compliance with GDPR	Implement appropriate data security measures e.g. data loss prevention
Conduct staff awareness training	Review and update privacy policies and data security arrangements	Implement age verification and gathering of parental/ guardian consent
	Establish procedures for data request, correction and removal	Implement appropriate system to manage and extract personal data
	Establish data breach plan	
	Conduct Privacy Impact Assessment	


Pin it
Analytics
business
data
science
analysis
decision
statistical
Statistics
based
mathematics
definition
field
use
Probability
patterns
practical
may
predicting
process
improving
choose
people
qualitative
fraud
using
understand
marketing
computation
include
strategy
involving
arrives
credit
erroneous
might
considered
historical
aspects
optimal
Operations
management
modeling
fields
applications
mining
making
performance
area
study
closely
eye
past
risk
i.e
make
includes
enterprise
managers
entity
realistic
extensive
limit
simple
order
Common
decisions
rules
holds
unless
involved
Also
term
predictive
simplest
Others
within
tends
thumb
discover
experiences
Research
denote
existing
future
resembles

Types of Data Analytics



Data Analytics – Tools

acl™

IDEA
Data Analysis Software

sas

Minitab

SPSS®

R

python™

Data Analytics – Approach

Step 1 Planning

Step 2 Data Preparation

Step 3 Analysis

Step 4 Reporting

Value of Data Analytics

A powerful tool that generally leads to significant improvements in productivity, efficiency, sales, profits and other key business metrics and goals.

Technology

Increase in computing power has advanced the technique of data analytics

Analytics

Harness big data analytics to deliver big value to business. By reducing complex data sets to actionable intelligence you can make more accurate business decisions.

Process

Using data can help companies improve their procurement efficiency, develop their marketing strategies, support business growth and, critically, differentiate themselves from competitors.

5 benefits of data analytics for business

Proactivity and anticipating needs

- Using customer data to under their needs to optimise customer experience and develop long standing relationships.

Delivering relevant products

- Anticipate market demands help companies stay competitive.

Personalisation and service

- Understanding customer attitudes and considering factors such as real-time location to help deliver personalisation in a multi-channel service environment.

Optimising and improving operational efficiency

- Apply analytics on business processes to optimise business operation for efficiency and effectiveness to fulfil customer expectations and achieve operational excellence.

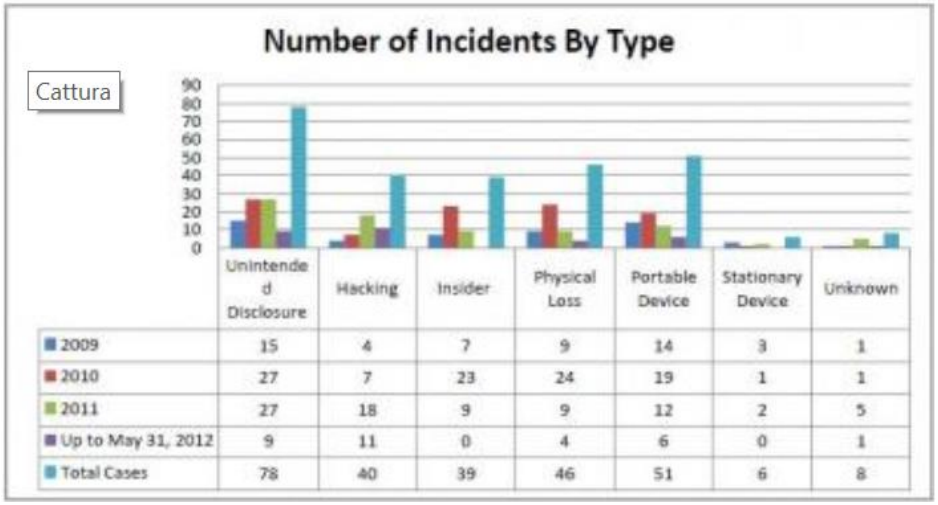
Mitigating risk and fraud

- Using fraud analytics to protect misuse of assets by internal and external threats.

Data Analytics – Sample use cases

IT incidents trend analysis

Detect and investigate recurring IT incidents.



Slow-moving inventory analysis

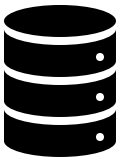
Detect excessive inventory due to slow-moving, dead and obsolete items.

(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)
ID	SKU#	DESCRIPTION	U/M	ON-HAND	UNIT COST	ON-HAND VALUE	ANNUAL USAGE	ANNUAL COST OF GOODS SOLD
1	A-45768	BODY CASTING	PC	76	$198.23	$15,065.48	200	$39,646
2	A-67324	DRIVE GEAR	PC	5	$12.34	$61.71	46	$568
3	D-45934	BOLT-3/8-20UNFC2.0	PC	326	$0.27	$86.72	500	$133
4	D-88346	WASHER-1/2 ZINC PL	PC	900	$0.03	$27.00	200	$6
5	X-45556	RESIN-PVC	KG	2566	$67.25	$172,563.50	66000	$4,438,500
6	X-85667	COLORANT-BLU	GAL	55	$59.60	$3,278.00	110	$6,556
						$191,082		$4,485,409
		Turnover= 23.5						

3 key takeaways

Cyber Risk

What can comprise your data?



Data

Protection

Why do you need to protect your data?

Analytics

Why and how to analysis your data?

Questions or comments?

How secure is my data?

What data policies do I need?

How do I use data analytics?

How do I classify my data?

I like to know more about …

Alvin Soh – Senior Manager, Risk Management
T +65 6329 2768
alvinsoh@moorestephens.com.sg