

# Risk Mitigation Strategies

National Cyber Security Summit

10 March 2010

ADVISORY

# Speaker

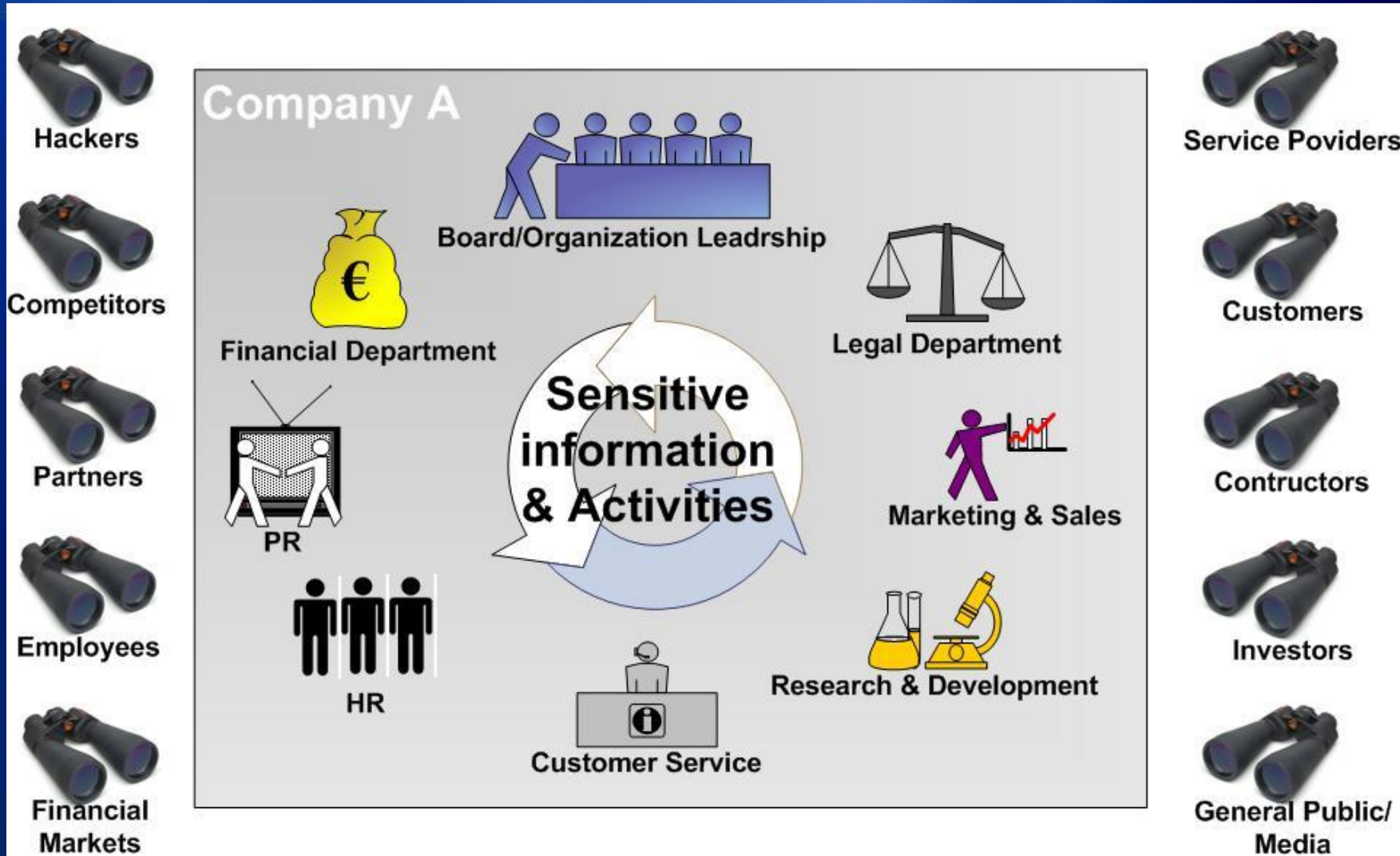
- **Reginald Nery, CPA, CISA, CISSP, CISM, CIA, CFSA, CCSA**  
**Head & Partner, Performance & Technology & Chief Information Officer**
  - Founding Director, member and Past President - Information Systems Audit and Control Association (ISACA) – Manila Chapter
  - Board member and Immediate Past President - The Institute of Internal Auditors – Philippines (IIAP)
  - Board member and Treasurer – Project Management Institute (PMI) – Philippine Chapter
  - Member, Philippine Institute of Certified Public Accountants (PICPA)
  - Member and Past Vice President for External Affairs, Association of Certified Public Accountants in Public Practice (ACPAPP)
  - Member, Institute of Electrical & Electronic Engineers (IEEE)
  - Member, International Information Systems Security Certification Consortium (ISC2)

# Risk Mitigation Strategy - Defined

A risk mitigation strategy is a organization's plan for how it will address its identified risks. Creating and implementing mitigation strategies is one of the most effective ways to protect an organization's information assets, and is nearly always more cost effective than repairing the damage after a security incident.

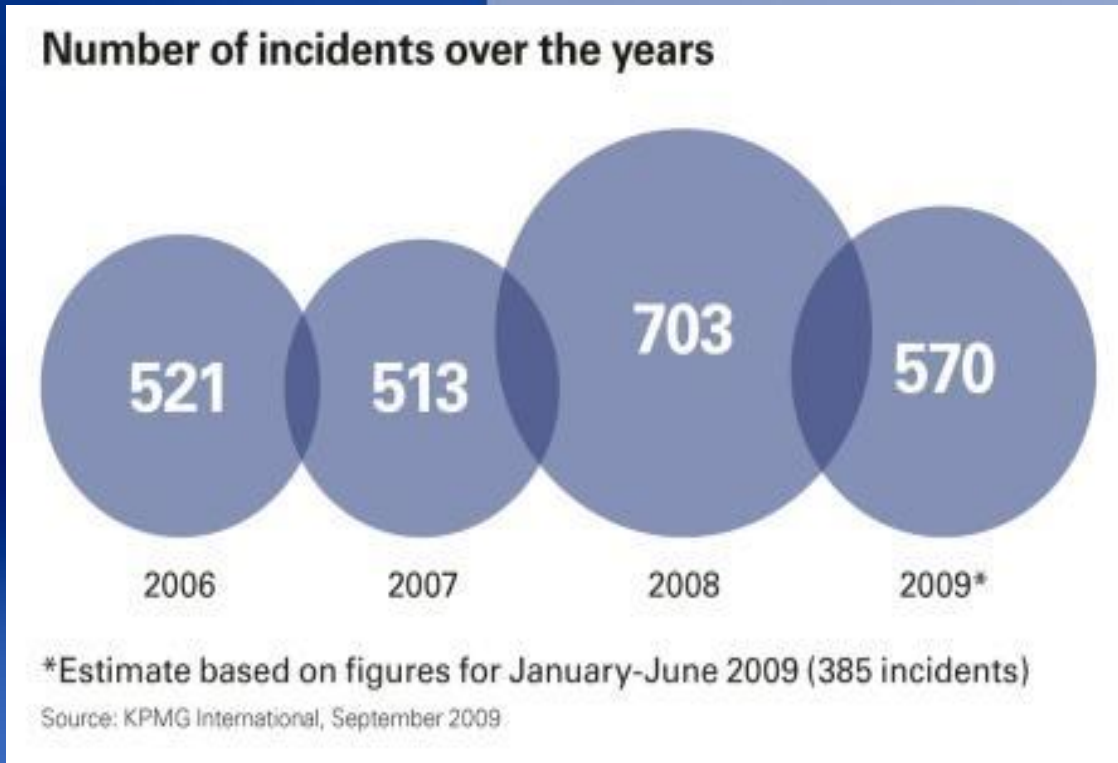
# Cyber Security

## The Challenge



# Data loss – The scale of the problem

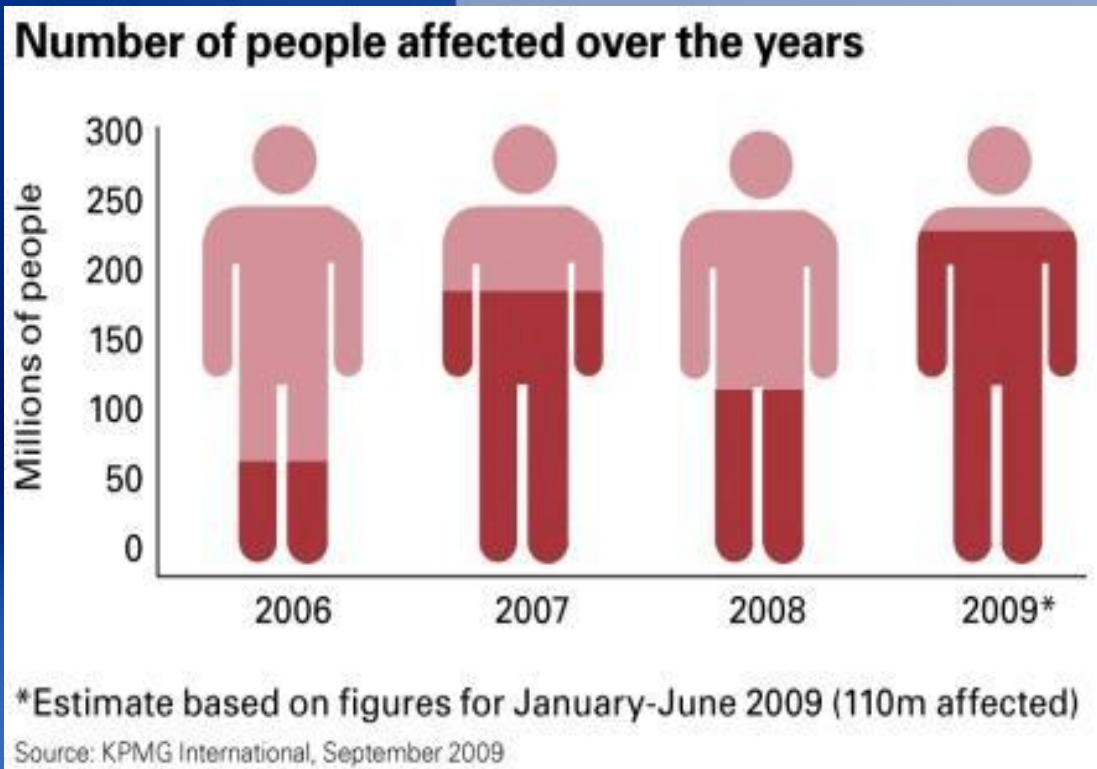
- Number of incidents over the years



- 2300 data loss incidents since 2005.
- Will we start to see more incidents due to emerging data breach regulations?

# Data loss – The scale of the problem

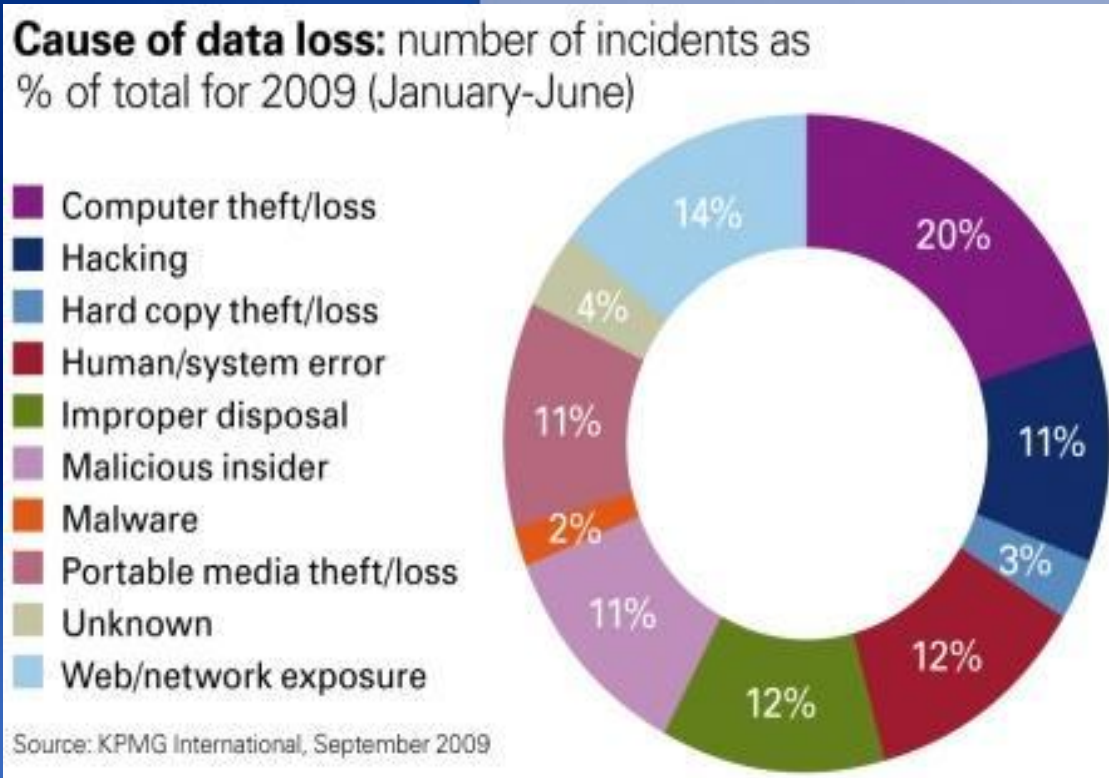
- Number of people affected over the years



- More than 700 million people affected since 2005.
- Over 100 million of those affected in 2009, were victims of the Heartland Payments Systems incident.

# Causes of data loss

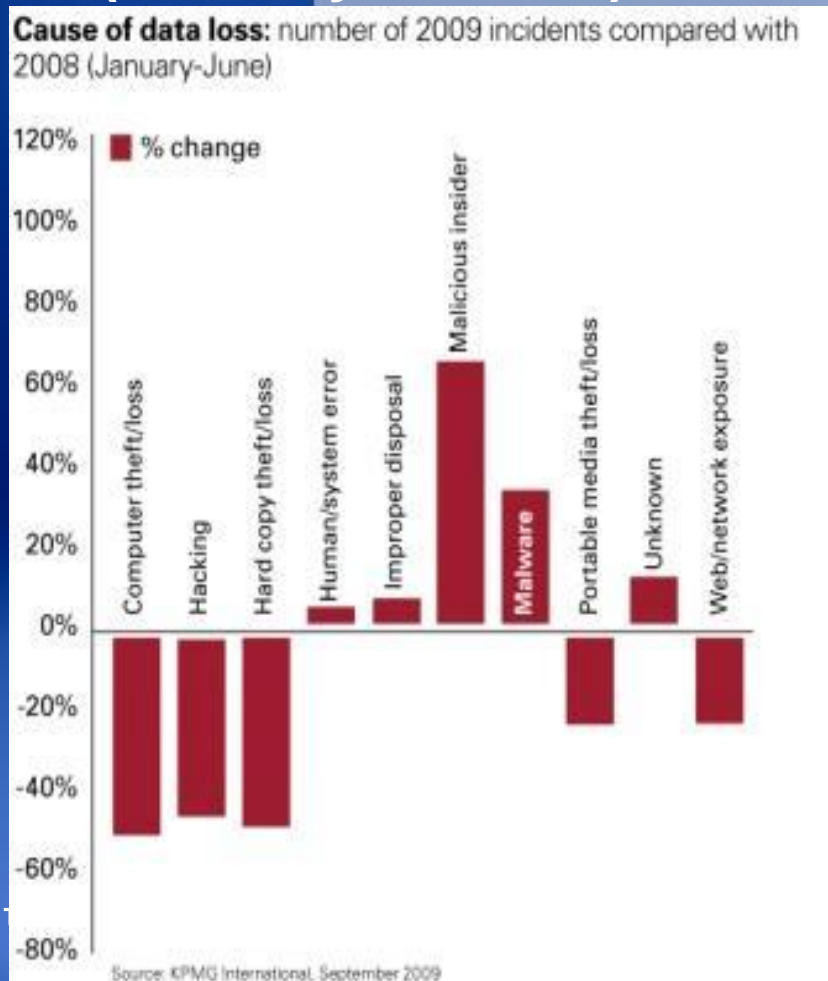
- Cause of data loss: number of incidents as % of total for 2009 (January – June)



- Safeguarding laptops should continue to be a key priority
- 14% of incidents are due to often inadvertent web or network exposures
- Disposal of hard copies and media should be addressed

# Causes of data loss

- Cause of data loss: number of 2009 incidents compared with 2008 (January to June)



- 68% increase in malicious insider incidents
- There are also rises in human/system error, improper disposal and virus incidents

# Causes of data loss

- Cause of data loss: number of people affected in 2009 (January – June)

**Cause of data loss:** people affected in 2009 (January-June)

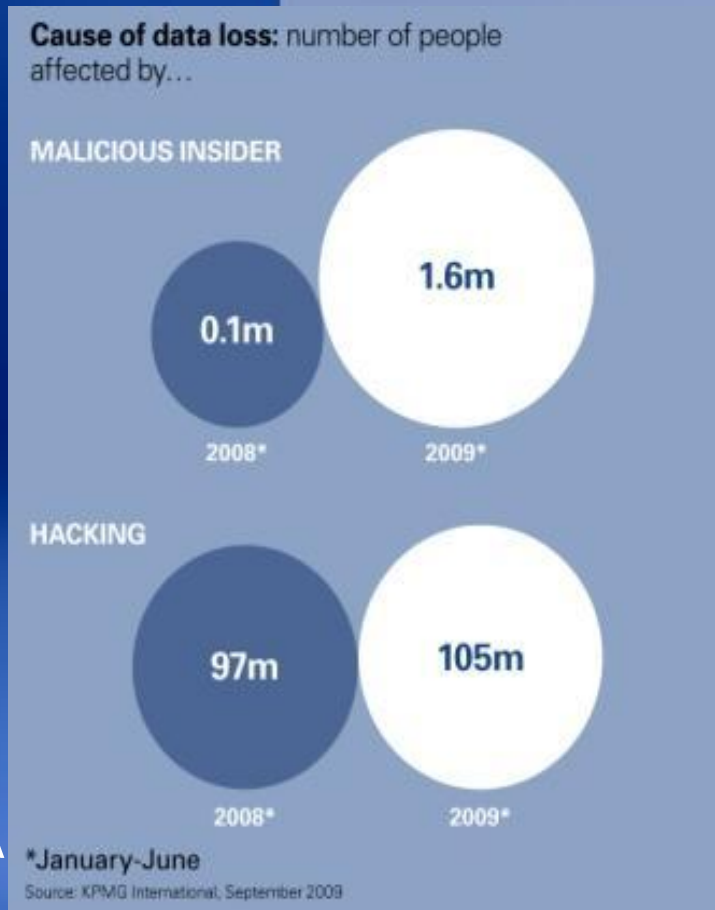
Incident type	No. of people affected
Computer theft/loss	2,081,422
Hacking	105,505,536
Hard copy theft/loss	11,960
Human/system error	291,417
Improper disposal	102,035
Malicious insider	1,555,148
Malware	34,567
Portable media theft/loss	1,340,995
Unknown	49,413
Web/network exposure	2,700,300

Source: KPMG International, September 2009.

- Almost 106 million records affected by hacking
- Almost 3 million records lost via web/network exposure

# Causes of data loss

- Cause of data loss: number of people affected by malicious insiders and hacking in 2009 (January – June)

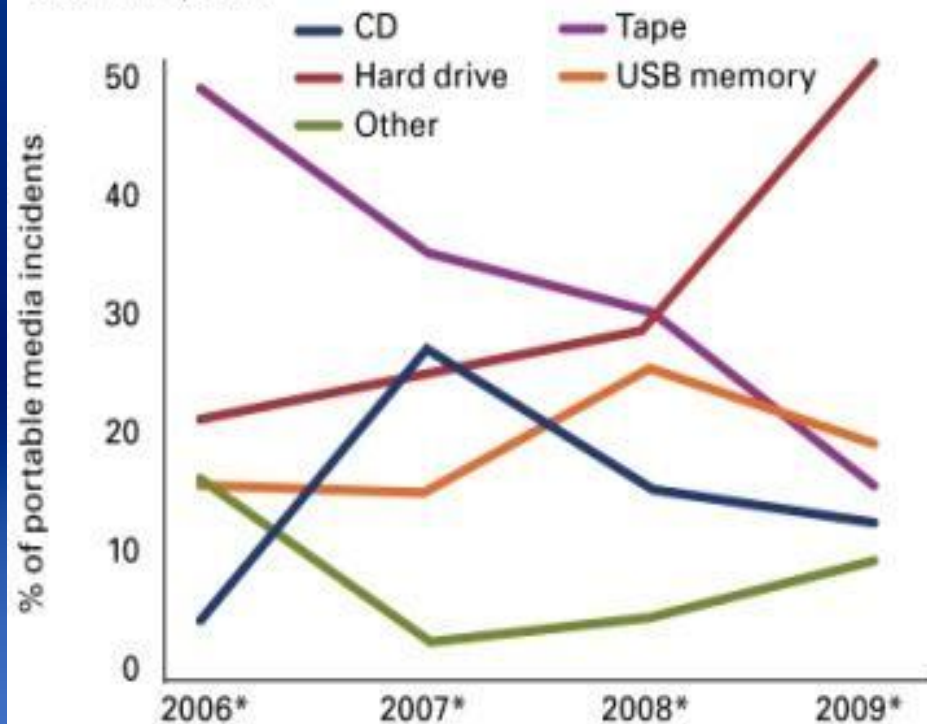


- Almost 1.6 million records revealed by malicious insiders
- Over 8% increase on number of people affected by hacking

# Data loss by portable media

- Data loss by portable media : number of incidents over the years

**Data loss by portable media:** number of incidents over the years



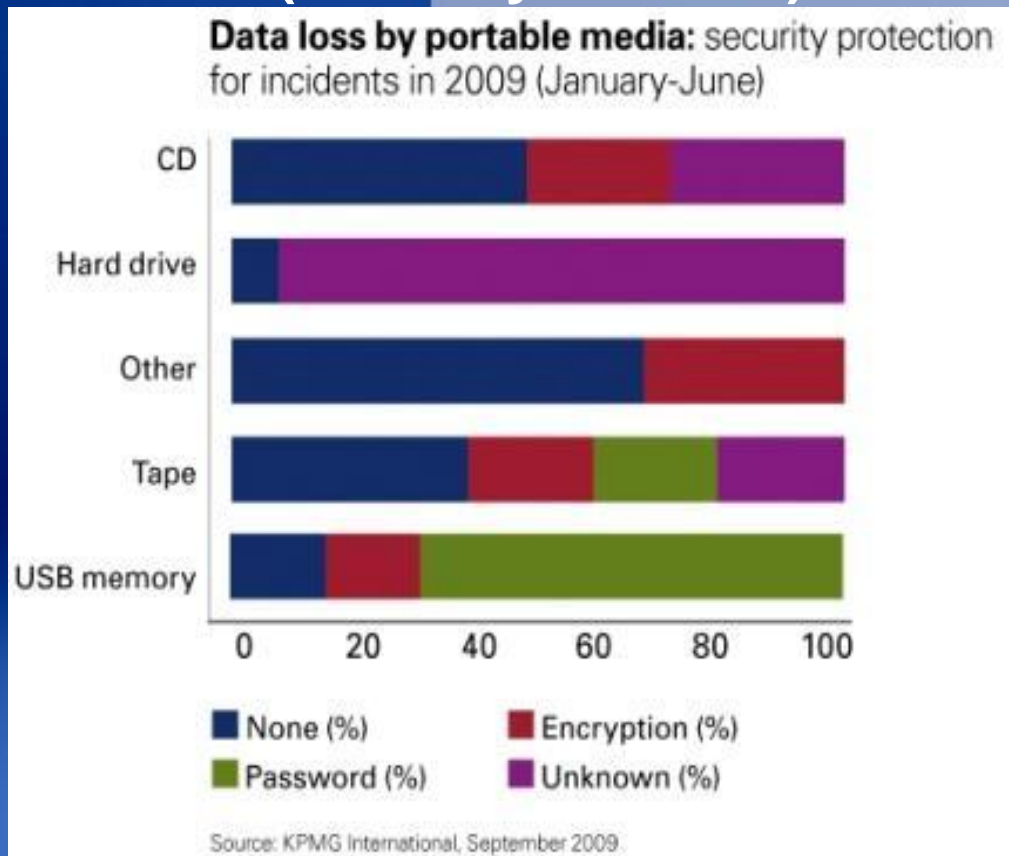
\*January-June

Source: KPMG International, September 2009

- Protecting external or internal hard drives should continue to be a key priority; as with USB memory sticks
- Data loss by tape is on a steady decline

# Data loss by portable media

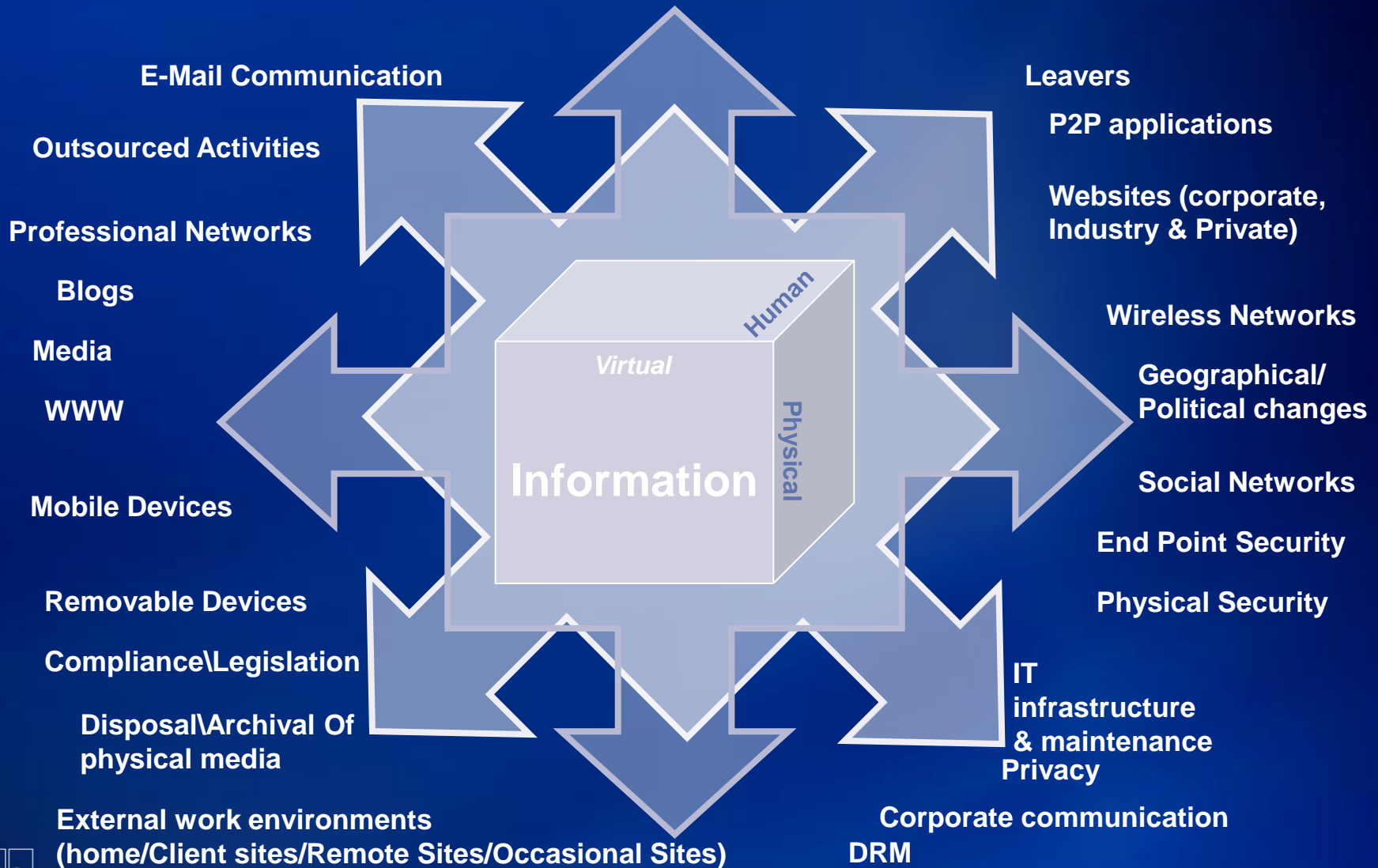
- **Data loss by portable media : security protection for incidents in 2009 (January to June)**



- Despite the ease of availability of encryption and authentication methods, data held within portable media are not protected
- Half of data loss via CDs were not encrypted or password protected

# Cyber Security

*Protecting Information In A Constantly Challenging Environment*



# Information Security Framework & Strategy

## Six critical elements of success for information security program implementation\*

1. Senior management commitment to information security initiatives
2. Management understanding of information security issues
3. Information security planning prior to implementation of new technologies
4. Integration between business and information security
5. Alignment of information security with the organization's objectives
6. Executive and line management ownership and accountability for implementing, monitoring and reporting on information security

# The 2009/2010 KPMG CISO Agenda

## Emerging Risks

- Intellectual Property Protection
- Targeted Malware Attacks
- Increased Data Leakage & Portability
- “Day Zero” Exploits
- Diverse Compliance Challenges
- Insider Risks
- Foreign National Threats
- Risk Management vs Risk Elimination
- Critical Infrastructure Protection
- Integration with ERM Initiatives

## Business Enablement

- Support for Rapidly Changing Business
- Focus on new Revenue Streams
- Mergers, Sourcing, Workforce Changes
- Increased Value Chain Integration
- Need for Improved Business Intelligence
- Globalization
- E-Discovery and Investigations

## Chief Information Security Officer

## Technical Architecture

- Virtualization
- “Cloud” Computing/SaaS
- IT GRC Solutions & Integration
- Data Leakage Protection
- SEIM Platforms and Programs
- IAM Governance (Role Optimization)
- Increased Encryption (Data Level & Portables)
- Application & Code Reviews
- Endpoint Security

## Security Management

- Better Integration with Board/ERM
- “Doing More with Less!”
- Vendor and 3<sup>rd</sup> Party Management
- Security Organization Model & Structure
- Asset & Configuration Management
- Executive Reporting & Metrics
- Managed Security Services
- Awareness & Training

# State of the Union – The New Realities

# 1

Increased Compliance Burden – More organizations are forced to spend more time focused on understanding and reacting to the changing Compliance environment than being proactive about Risk Identification and Management.

- New/Updated Laws & Regulations
- Third Party Relationships
- Government Investment

# 2

Changing Threat Vectors – Security threats continue to evolve in new and unexpected ways.

- Broad evolution of mal-ware
- Targeted attacks
- Insider Threats

# 3

Global Economic Crisis – The crisis has created a rapid evolution in business models and reprioritization across all aspects of the business.

- New delivery channels & business arrangements
- Monetize existing assets (including data & information assets)

# Key Drivers for Information Protection (Now)



# Enterprise View of Risk and Control Value

## Business Risk Drivers

- Information protection functions will be asked to reduce the cost of providing control and assurance without reducing the level of asset protection. Increased integration in Operational Risk functions.
- Current control models often assume a one-size-fits-all approach, requiring the highest level of protection for all information assets, significantly increasing the cost of control.

## Protection Strategies

- Evaluate and assign protection requirements to business processes, utilizing risk metrics such as the presence of regulated data, business impact, and findings of previous risk assessment activities.
- Build and maintain enterprise dashboards for consolidating risk management activities and providing a centralized view of risk factors across the organization.

## Key Considerations

- Extend existing asset management capabilities beyond operational roles to include asset risk prioritization and cross references to security information such as threat, vulnerability, and incident management.
- Include vendors, contractors, and other third parties in risk assessment programs to understand, restrict, and control their use of the organization's sensitive and protected information.

# Changes in Business Models

## Business Risk Drivers

- Organizations are entering new markets rapidly, both from a geographic perspective as well as through adjacent businesses, incurring additional regulations.
- Divestitures are occurring with more frequency and speed than previously, requiring the ability to segregate sensitive systems quickly.
- Enterprises will rely more heavily on economies of scale achieved through outsourcing and the use of third party vendors.

## Protection Strategies

- Implement a security-focused vendor management program, including the development of score cards, assessment methodologies, and a model for placing vendors into tiers based on risk and business value.
- Assess organizational use of cloud computing, virtualization, and outsourced computing models, focusing on creating zones of trust and protection requirements for information assets stored or processed by third parties.

## Key Considerations

- Examine information protection processes for opportunities to leverage third party service providers in performing routine or non-business focused tasks such as security device management.

# Targeted Attacks

## Business Risk Drivers

- Organizations are under scrutiny from multiple regulatory bodies regarding the protection of customer information and related IP.
- Increased use of customer information for marketing, sales, and product refinement drives an increase in the scope of information protection requirements for sensitive items like financial & health data.
- Laptop and PC loss and theft accounted for over half of data breaches in 2007 and 2008.

## Protection Strategies

- Update information security awareness training programs to address these new threat vectors, specifically phishing tactics and other social engineering-based attacks.
- Evaluate current technology controls for malware protection, hard disk encryption, network location awareness tools and host-based intrusion prevention to address the potential for attacks on mobile clients.

## Key Considerations

- Consider the use of security-in-the-cloud providers as a potential source of protecting end-points, particularly mobile devices.
- Utilize existing content restriction tools and infrastructure to prevent access to potentially-malicious sites and locations on high-value end-points.

# Increased Insider Risk

## Business Risk Drivers

- Insiders account for a majority of information security breaches, a trend likely to increase as employees and contractors face lay-offs and shutdowns.
- Heightened demands for productivity will result in operational risk increases, particularly in cases where previous control mechanisms have slowed processes or reduced efficiency.

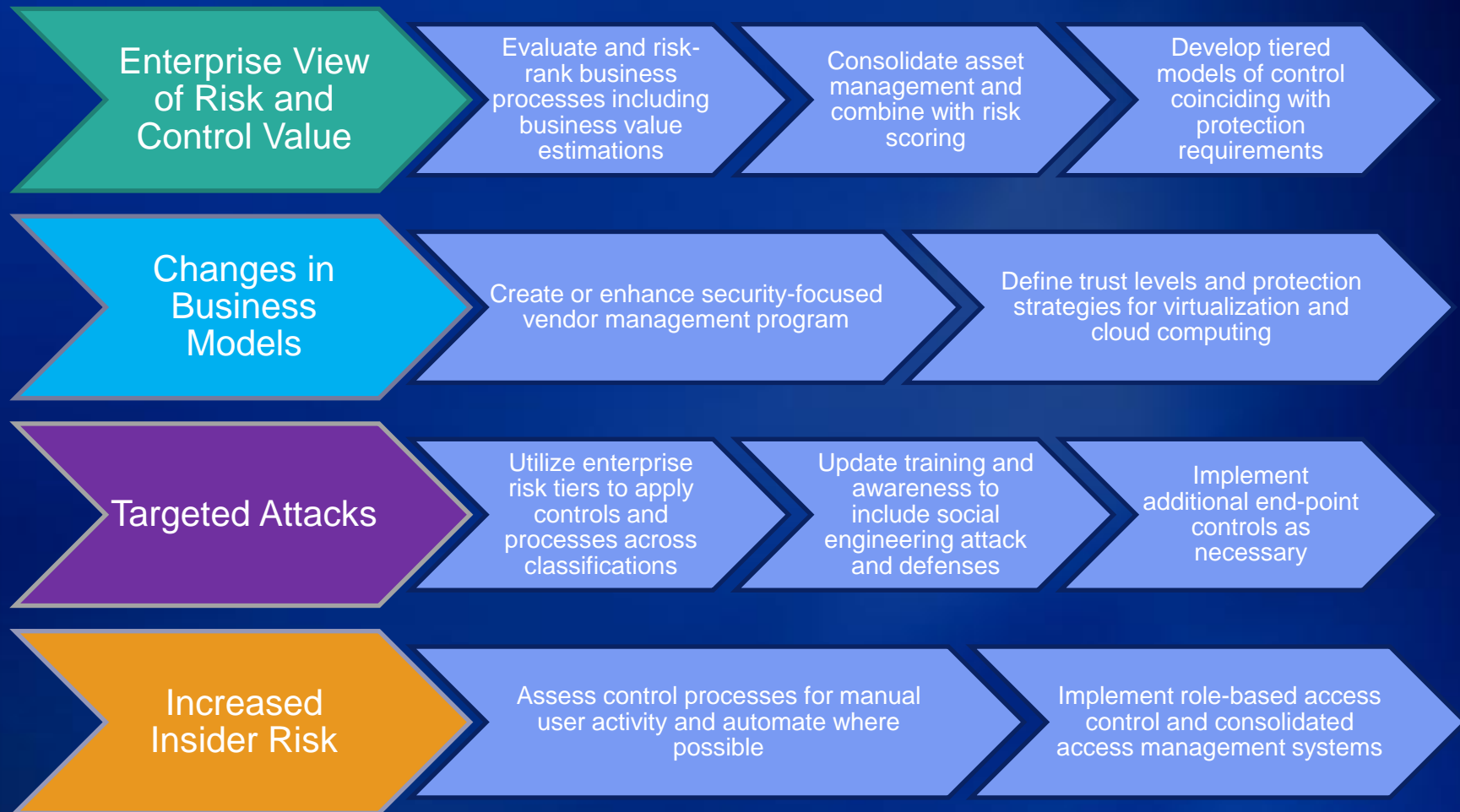
## Protection Strategies

- Consolidate access management systems, leveraging business use information and protection requirements to create and implement role-based access controls.
- Evaluate existing control portfolio for information protection controls that rely on user interaction, seeking alternatives to leverage automation where possible and reduce process impedance.

## Key Considerations

- Prioritize assessment and control activities based on divisions facing the largest scales of personnel changes and where employees or contractors have access to sensitive information.

# 2010 Project Roadmap and Agenda



# 2009 Wrap-Up

**As a year in information protection, 2009 was momentous as it saw the maturation of several long-coming security themes:**

- Targeted malware, used in advanced persistent threat attacks, compromised some of the best-known companies in the world;
- Faced with one of the most challenging business environments in recent memory, companies shifted operating models and faced significant changes in regulation;
- Information security organizations deployed automated tools to address compliance burdens, while providing new transparency to business partners;
- From new unified toolkits to consolidation of security leadership roles between physical, fraud, and information, “convergence” was the buzzword most heard.

**Advances made in protecting our enterprise assets in 2009 were considerable, particularly given the budgetary challenges most organizations faced in a very difficult environment. However, the advances observed in the threat environment mean there is much more to be done in 2010 and beyond.**

# User Maturity

## Business Drivers

- Many end-users, customers, and third parties are technology-savvy and regularly use a collection of advanced computing capability, including smart phones, e-readers, tablet PCs, netbooks, and alternative software suites.
- The same features that make these technologies attractive for personal use inspire their use in a business setting, typically outside the realm of control by IT.

## Strategies

- Focus on the protection of the company's information assets and sensitive business functions, whether they are in use on a company-owned (and managed) processing asset or not.
- The use of centrally-controlled "sandboxes," in some cases through endpoint virtualization technologies, can promote the protection of sensitive enterprise data while enabling a vast array of user-provided devices and platforms.

## Key Considerations

- A strong understanding of the devices in use on all segments of the enterprise network is a prerequisite to gaining insight into alternative use cases.
- Rather than preventing users' desire to increase productivity, information security groups must identify and support these alternative use cases where possible.

# Operational Compliance

## Business Drivers

- The demands of new compliance mandates are increasing annually and typically at a rate beyond what the information security organization of most companies can address with the resources available.
- Operational stakeholders – system administrators, process owners – are enduring more and more visits from compliance-related auditors and security personnel.

## Strategies

- Based on an enterprise risk assessment, select and implement a unified control framework to address all information technology compliance mandates and assign ownership for the specific objectives and controls to operational owners outside of the information security organization.
- Enable control and process owners to self-assess their control and compliance requirements, using a common testing procedure across business units and divisions.

## Key Considerations

- By building a unified testing approach, and by pushing the test activities to the control owners, efficiencies are gained and the depth of compliance testing can be expanded.
- Automated controls testing can be enabled through the use of existing vulnerability scanning infrastructure as well as the addition of business-logic controls testing platforms.
- Workflow automation engines enable these processes without introducing additional personnel overhead. Many of the modern GRC platforms provide building blocks for enabling this approach.

# Data Ownership

## Business Drivers

- New application delivery models have emerged in the form of Software-as-a-Service and now providers are building Infrastructure- and Platform-as-a-Service capabilities to tap into the market interest in Cloud Computing.
- Enterprise information stored, processed or transmitted to and from these systems may still be subject to regulatory oversight as well as internal protection requirements.

## Strategies

- In order to leverage the attractive cost models and capabilities provided by alternative delivery methods, data ownership must be established at the business level, requiring that organizations understand the current information architecture of applications and platforms prior to a migration.
- Emerging technologies utilizing tokenization and in-channel transparent encryption of data on its way out of the organization may address many security-related concerns.

## Key Considerations

- The challenges of Cloud Computing are not new; shared data processing facilities already perform the bulk of transactional processing for many organizations today (consider fractional mainframes, outsourced payroll, and managed service centers).
- Many countries now limit the types of information about citizens that can be shared outside of the home country. Organizations implementing cloud security should carefully identify these risks.

# Threat Targeting

## Business Drivers

- Many organizations have considered information protection a low risk area, as the data they handle isn't one of the traditional targets for opportunistic hackers – financial services, critical infrastructure.
- With the emergence of advanced persistent threats (APT) – attackers focused on a handful of organizations for a very long period of time – threat targeting has broadened to include organizations that may offer nothing more than a stepping stone to an ultimate target.

## Strategies

- Identifying APT attacks can be very difficult using traditional technologies in silos; often, the malware and attack vectors used are not publically-known, meaning no protection mechanisms are in place.
- Correlating between multiple systems – security infrastructure such as IDS and antivirus, operational log data, and continuous auditing systems – may enable the detection of an attacker's presence.

## Key Considerations

- Technologies are available to assist with performing the correlative actions, but a significant amount of process design must be completed first. An organization must understand the criticality of the systems they are monitoring, a triage process for responding to incidents, and an appropriate handling process during an incident.
- Incident and event data should be used to improve the organization's risk assessment processes.

# Recap:

## Security assessment and assurance

- Organizations need to understand and identify weaknesses in their information handling systems and processes. You may avail yourself of third-party services ranging from in-depth technical reviews of IT systems, to external and internal penetration tests, to evaluations of governance and policy arrangements. Understanding where you are most vulnerable is key to actively managing the risks you face and reducing the chances of data loss.

# Recap:

## Incident management

- Organizations need to assess, manage and respond to the consequences of data loss. In case of incident, there's a need to confirm the extent of the breach and assess how likely it is that the lost data will be used fraudulently. Organization needs to notify relevant authorities and affected customers, to define and implement recovery strategies, and to collaborate with regulators and legal advisors.

# Recap:

## Awareness and training

- Organizations need to improve their employees' security awareness and handling of confidential information. Based on our years of experience with other organisations, we believe that behavioural change programmes need to be devised to enable staff and key suppliers to understand and fulfil their individual responsibilities for protecting critical data. An awareness and understanding of how to respond when something goes wrong is a very important element of security strategy.

# Questions and Answers



# Contact Information

Reginald C. Nery, **Head & Partner**

Performance and Technology/ Information  
Protection & Business Resilience

Manabat Sanagustin & Co.

The KPMG Center

6787 Ayala Avenue

Makati City 1226, Philippines

Phone +63 2 885 7000 ext: 207

D.L +63 2 885 0607

Mobile +63 917 577 5296

Fax +63 2 816 6595

+63 2 894 1985

Email: [rcnery@kpmg.com](mailto:rcnery@kpmg.com)