Global Trends in Information Security Risk Management and the Greek Perspective

02 December 2011

Gregorios Themistocleous | CISA, CRISC, ITIL
Senior Manager
Gregorios.Themistocleous@gr.ey.com

Ernst & Young
Quality In Everything We Do

ISACA
Trust in, and value from, information systems
Athens Chapter

Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Ernst & Young's 2011 Global Information Security Survey

- Longest running, most recognized and respected annual survey of its kind
- Interviews with 1,700 IT and information security executives globally
- 52 countries, across multiple industry sectors

Information security is still one of the most important issues facing organizations today

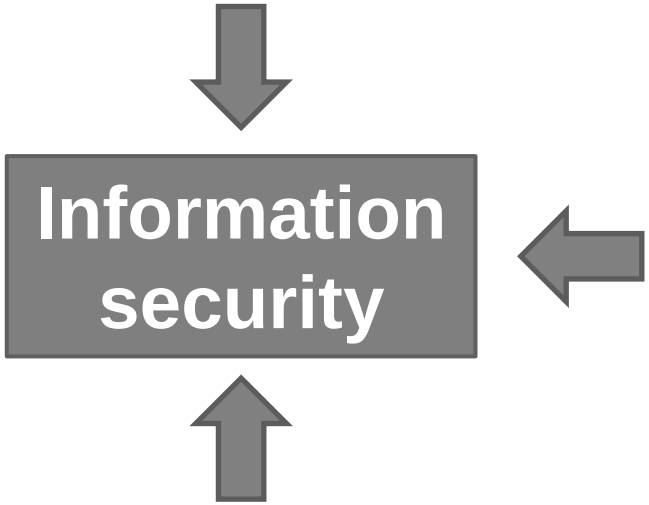
Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Today's IT trends affecting information security

Digitization

- Tangible products are becoming software
- Technologies transform entire industries



Moving into the cloud:

- From outsourcing to the cloud
- Transformation of IT departments

Borderless environment

- Anytime, anywhere access to data
- Mobile computing & social media

What is happening to information security today

- Risk trends
  - 72% of respondents see an increasing level of risk due to increased external threats
  - 46% of respondents see an increasing level of risk due to increased internal vulnerabilities
  - 21% of respondents see a decreasing level of risk due to decreased internal vulnerabilities
  - 9% of respondents see a decreasing level of risk due to decreased external threats

Coming out of the fog

- Information security is a critical component and key enabler for successful transition to the cloud
  - 52% of respondents have a documented information security strategy
  - 12% of respondents present information security topics at board meetings
  - 51% of respondents believe that the information security function is not meeting the needs of their organization
  - 59% of respondents say that their information security budget will increase in the coming year

Perspectives

- Bring information security into the boardroom
- Make information security an integral part of service and product delivery and everyone's day to day thinking
- Focus information security on protecting what matters most
  - Customer information
  - Intellectual property

Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Staying connected

Cloud computing, mobile & social media

- Survey results – cloud computing
  - 61% of respondents are currently using, evaluating or planning to use cloud computing-based services within the next year
  - 48% of respondents see the implementation of cloud computing either a difficult or very difficult challenge
  - 52% of organizations have not implemented controls to mitigate new risks related to the use of the cloud
  - 90% of respondents believe that external certification would increase their trust in cloud computing

Staying connected

Cloud computing, mobile & social media

- Cloud computing risks and challenges
  - Compliance and privacy
  - Information security and data integrity
  - Contract and legal
  - Governance, risk management and assurance
  - Reliability and continuity of operations
  - Integration and interoperability
  - Impact of ever-changing regulations

Staying connected

Cloud computing, mobile & social media

- Survey results – mobile
  - 80% of organizations are either using, evaluating or planning to use tablets in their business
  - 57% of respondents have made policy adjustments to mitigate the risks related to mobile computing risks
- The most frequently taken measures to mitigate risks related to mobile computing
  - 57% policy adjustments
  - 52% security awareness activities

Staying connected

Cloud computing, mobile & social media

- Survey results – social media
  - 40% of respondents rated social media-related issues as either challenging or significantly challenging
- The most frequently taken measures to mitigate risks related to social media
  - 53% ‘limited’ or ‘no access’ to social media sites
  - 46% policy adjustments

Perspectives

- Cloud computing
  - Trust, but verify
  - Plan for continuity and select providers that are transparent about resiliency build back ups and test recoverability
  - Use standard security processes and techniques that have worked in the past
  - Align business and information security strategies
- Mobile
  - Establish governance and guidance for the use of mobile devices and products
  - Use encryption as a fundamental control
  - Perform attack and penetration testing on mobile apps prior to deployment
- Social media
  - Reevaluate the use of hard-and-fast ‘no access/no use’ policies
  - Embrace the full advantages of social media

Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Preparing for the worst
Business continuity management

- Survey results
  - For the next consecutive year, respondents have identified business continuity management (BCM) as their top funding priority
  - 18% of organizations do not have a BCM program in place
  - 47% of respondents find their BCM program well documented and robust
  - 55% of respondents have a BCM program that is approved by management
  - 55% of respondents have procedures in place to protect their organizations' people

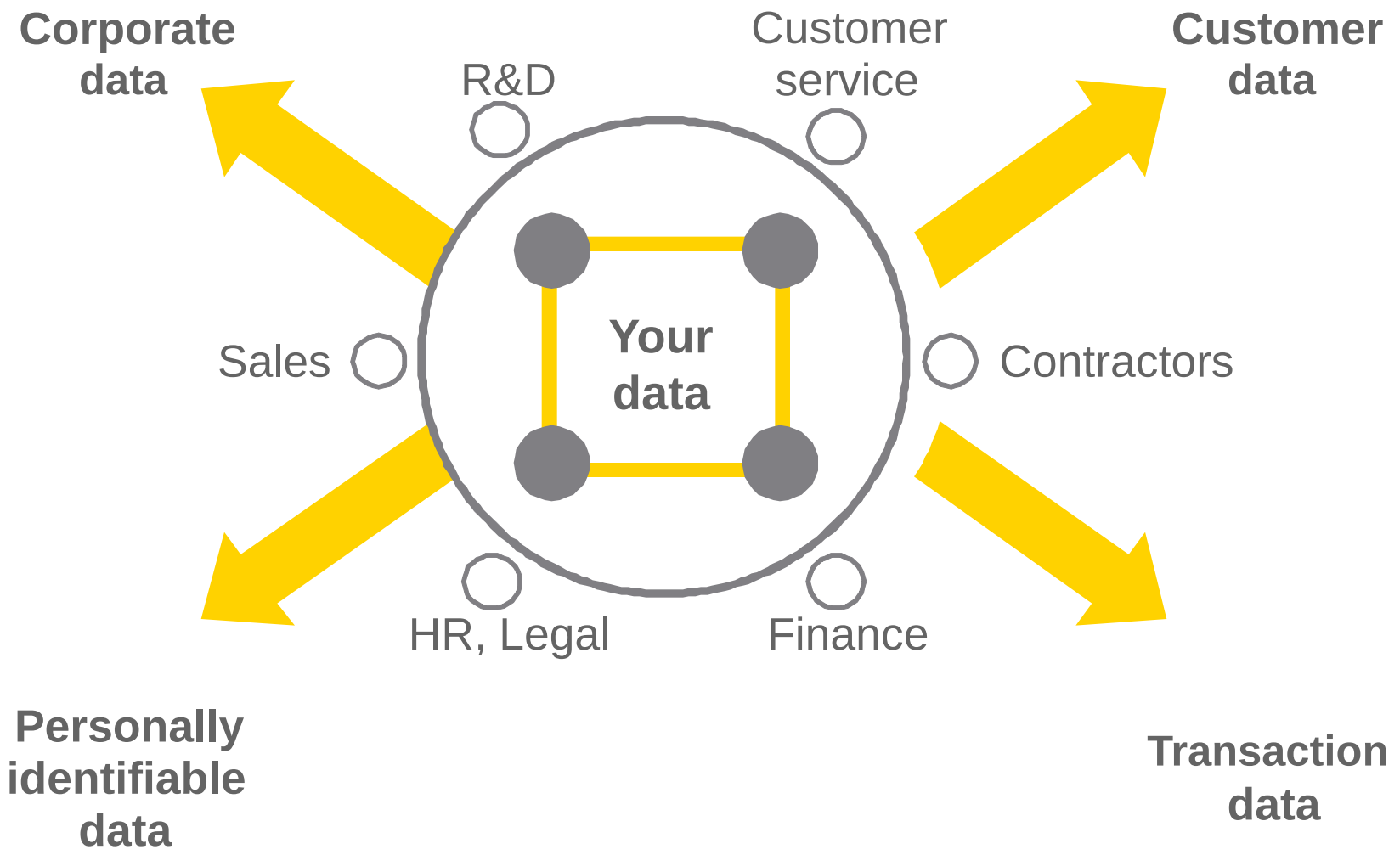
Perspectives

- Prepare for and secure business continuity plans that anticipate high-impact, low-frequency events, and determine which are integrated into a broader risk management framework that focuses on protecting an organization from catastrophic loss
- Assess whether the business continuity plan has the right level of maturity in light of emerging trends
- Test the business continuity plan frequently. The more complex the scenarios, the better.
- Solicit the support of the board and audit committee

Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Plugging the data leaks



Facts about data leakage

- The average organizational cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record, markedly higher when compared to $204 in 2009*
- There are now many more ways data can leave an organization (mobile, social media etc.).
- The sheer volume of data is increasing as ever before

* *"2010 Annual Study: U.S. Cost of a Data Breach" Ponemon Institute and Symantec*

Data leakage (malicious)
Examples

Root cause	Data category	Case description
Inappropriate access rights to applications with sensitive data	Customer data	A frustrated staff member used the standard data export procedures to export sensitive data and copied it to a CD.
Employee discontent	Corporate data	An employee accessed the customer master file and exported it to an Excel file. This file was then emailed to the employee's personal email account.
Insider trading	Corporate data	An employee with access to pre-released financial information fed information to an external analyst, resulting in improper stock trades for both the employee and the analyst.

Plugging the data leaks

- Survey results
  - 66% of organizations have not implemented data leakage prevention tools
- The two most frequently taken measures to mitigate risks related to data loss
  - Defining a policy for handling sensitive information
  - Employee awareness program

Security trends
Countering cyber attacks

APT attacks are focused on a single target, lasting until they are in, and are meant to collect information over a long period of time.

They leave few signs of their success, stay hidden for as long as possible to acquire large amounts of sensitive information.

- No single technology or process will stop the advanced persistent threat (APT)
- Traditional security methods are proving to be ineffective against APT
- Many organizations are vulnerable to attack because they have under-invested in security
- Existing and conventional defenses is not enough; new approaches and increased vigilance are required
- Protecting against these types of threats requires several layers of defense, and advanced knowledge and skills to detect and react to ongoing/successful attacks

Security trends
APT: Who is a target?

The APT collects information from a specific group of organizations.

The population of target victims has clearly grown over the last several years, and the attackers will use any means possible to exploit the target.

Target industries	Motivation
Government contractors	• Theft of intellectual property (e.g., equipment test data) • Theft of government classified Information
Technology providers	• Theft of intellectual property to bring competing products to market with less R&D time and investment • Theft of corporate secrets to gain competitive advantage in negotiating contract and buying terms
Manufacturing	• Theft of intellectual property to bring competing products to market with less R&D time and investment • Theft of corporate secrets to gain competitive advantage in negotiating contract and buying terms

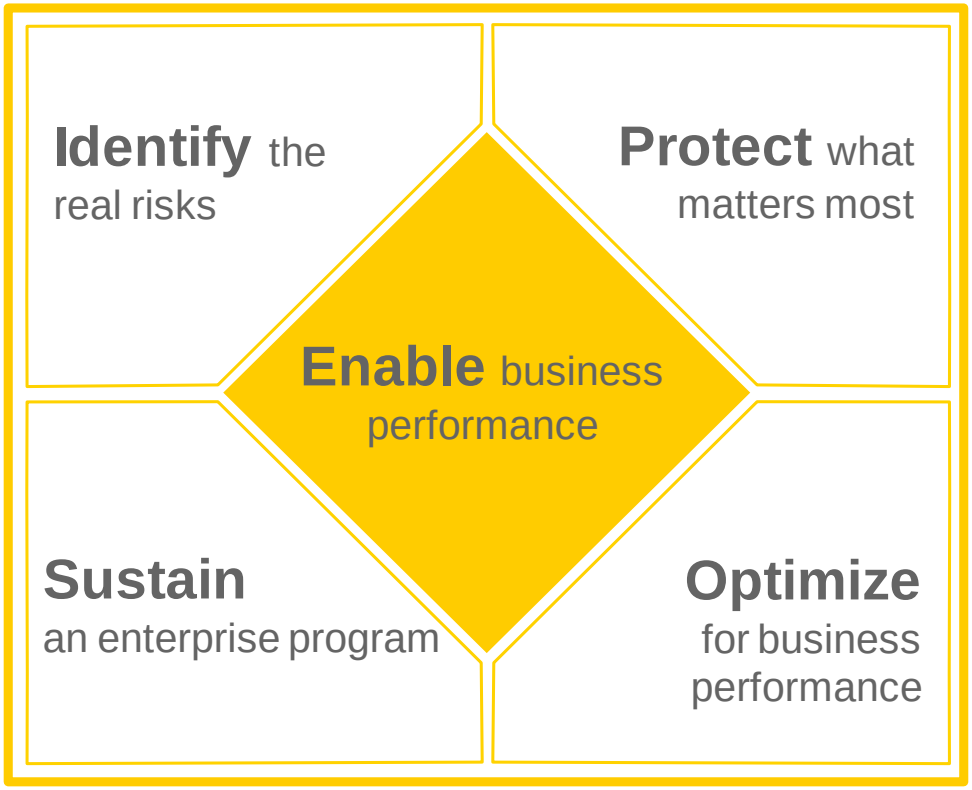
Perspectives

- Assess, understand and appreciate the potential risks and areas of data loss, ranking the risks
- Identify, assess and classify sensitive data across the enterprise
- Take a holistic view of data loss prevention by identifying key DLP controls and measuring their effectiveness
- Cover data in motion, data at rest and data in use
- Implement incident investigation
- Pay special attention to third parties with access to sensitive company data
- Understand what data is sent to third parties, how it is sent and if the transmission mechanisms are secure

Today's Agenda

- Moving into the cloud and out of the fog
- Staying connected: cloud, mobile & social media
- Preparing for the worst: business continuity
- Plugging the data leaks
- Looking into the future

Transforming your information security program



Five questions for the C-suite

- **Do you know how much damage a security breach can do to your reputation or brand?**
- **Are internal and external threats considered when aligning your security strategy to your risk management efforts?**
- **How do you align key risk priorities in relation to your spending?**
- **Do you understand your risk appetite and how it allows you to take controlled risks?**
- **How does your IT risk management strategy support your overall business strategy?**

Looking into the future

- Revisit your information security strategy to conform to the current landscape risk
- Instead of acquiring the latest tools, focus on the fundamentals
- Implement a structured, pragmatic approach to managing IT risk, focusing on risks that matters
- Address the issue as a business risk, broader than just IT

Related thought leadership

- **For additional material and thought leadership visit: www.ey.com/informationsecurity**

Questions & Answers

THANK YOU

Global Trends in Information Security Risk Management and the Greek Perspective

02 December 2011

Gregorios Themistocleous | CISA, CRISC, ITIL
Senior Manager
Gregorios.Themistocleous@gr.ey.com

ERNST & YOUNG
Quality In Everything We Do

ISACA
Trust in, and value from, information systems
Athens Chapter