IT Security Risk in the Business Environment

A layered approach to information security risk

Presented by:
Garfield Reece, Partner, PricewaterhouseCoopers
Hugh Thompson, S. Manager, PricewaterhouseCoopers

GARP Global Association of Risk Professionals

Agenda

Our discussion will aim to cover the following:

- Brief introduction to the IT Business Risk model
- Understanding information technology security risks within the business environment
- Applying a ‘Defense-In-Depth’ approach in understanding IT security risks
- Overview of the risks at the different security layers.

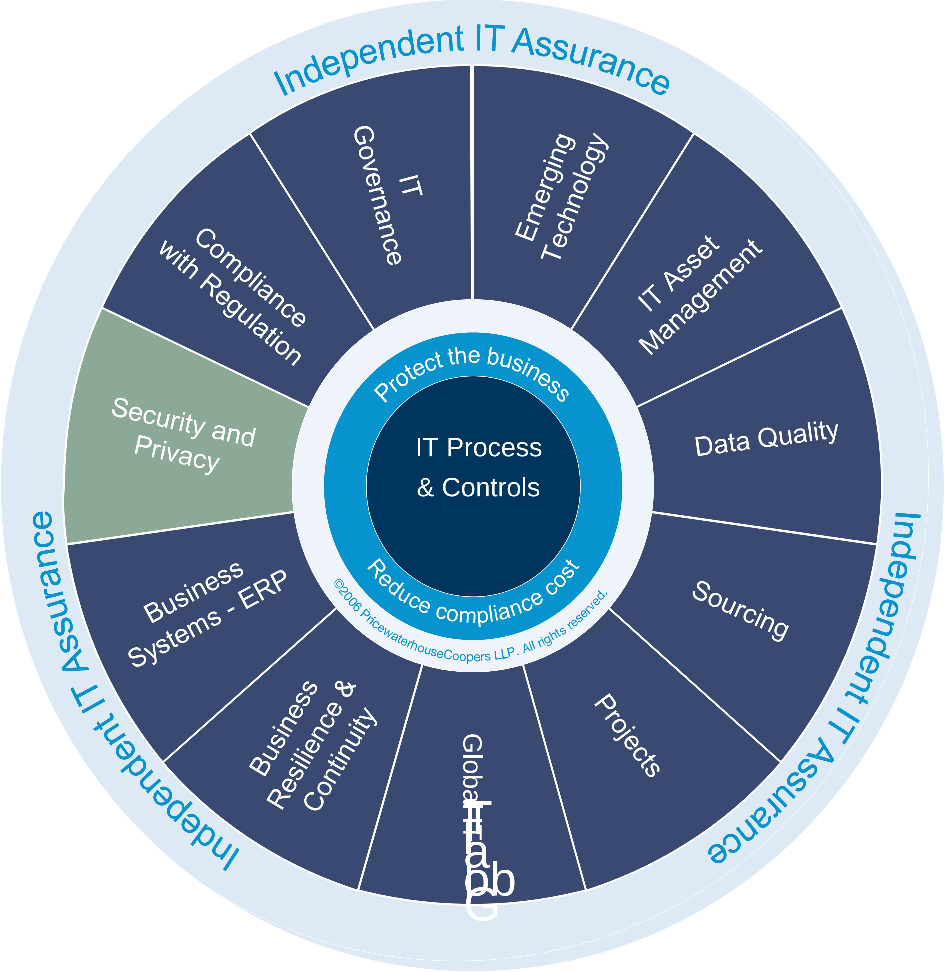
Introduction

There are several IT risks that are on the Board’s and the Audit Committee’s agenda. The impact of these risks is both operational and financial in nature and as such represent a key area of focus for both IT and Financial management.

The IT Business Risk Drivers model captures the significant IT risks.

IT Business Risk Drivers Model

The technology risk universe can be thought of as 11 distinctive areas that drive risk within an organization.



©2006 PricewaterhouseCoopers LLP. All rights reserved.

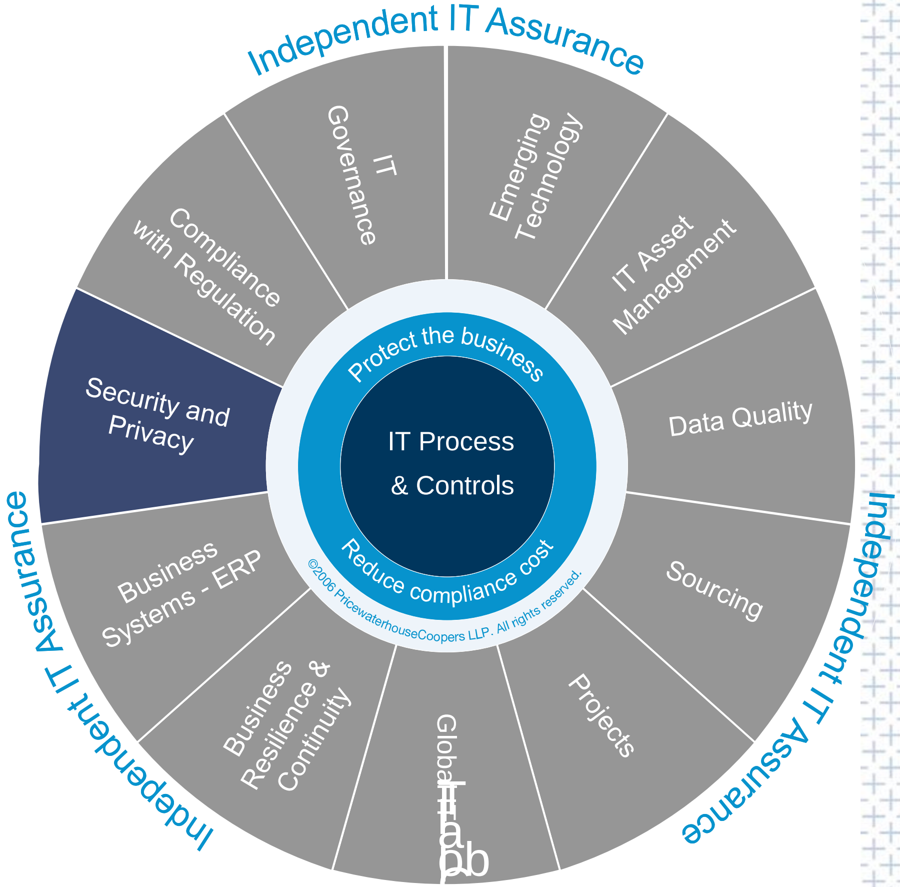
IT Business Risk Drivers Model – Security and Privacy

Why is this area important?

- Information is one of the most valuable assets an organization possesses, it needs an appropriate level of protection.
- An information security breach can be devastating to reputation which can have a direct impact on future revenue.
- Regulatory obligations highlight the Audit Committee's need to focus on this area.
- 75% of US & UK businesses rate security as a high or very high priority.
- More than 60% of companies report that there will be more, harder to detect, security incidents in the future

What can go wrong?

- Company, employee and customers information and data may be compromised (Target security breach, First Caribbean and Edward Snowden).
- Information or data may be lost or destroyed.
- Information systems and services may become unavailable (DoS attacks).
- Financial losses due to fines, lawsuits and reputational impact.
- Everyday, there are security breach attempts. It is just a matter of time…



The Current Business Environment

IT security risk is one of the key risk drivers in todays business environment. This is because technology is at the forefront of business development for future and sustainable growth. We see this in many ways, for example:

- Growth in e-commerce sales, which are out-pacing brick-and-mortar sales.
- Growth in mobile computing (e.g. smart phones, tablets, notebooks, 4G data speeds, etc.) where employees want access to information and systems from anywhere.
- Customers need for on-demand access to information and services around the clock (e.g. On-line banking, on-line bill payment, online phone card top-up, transaction statements, etc.).
- Need for businesses to find more cost effective ways to expand it’s IT infrastructure while lowering cost (e.g. Infrastructure, software services and data storage in the in cloud).
- Business process automation (order to cash and procure to payment) which reduces the need to maintain paper trails.
- Companies need to use social media for marketing and to connect with customers and employees.

The Current Business Environment and Key IT Risk Drivers

This has however introduced the following risks within the business environment:

- Access risk – The risk that systems, information and data may be accessed, maliciously or accidentally by unauthorised individuals.
- Availability Risk – The risk that systems, information and data may be lost and/or not be available as required.
- Integrity Risk – The risk that business application may not function as intended or in-line within management’s objectives.

In addition, the move towards attaining greater efficiency, market exposure, client interaction and cost reduction, companies will adopt to emerging technologies. However, this has introduced additional risks, for example:

- Third-Party Risk – The risk exposures which may impact a business as a result of the outsourcing of a process to a service provider .This risk represent a accumulation of all other risks; however, this risk reside at the third-party service provider.
- Social Media Risk – The risks users and companies are exposed to as a result of having a social presence.
- Mobile Security Risks – The risks introduced to a business by persons using mobile devices (e.g. smart phones and tablets) in the business environment.

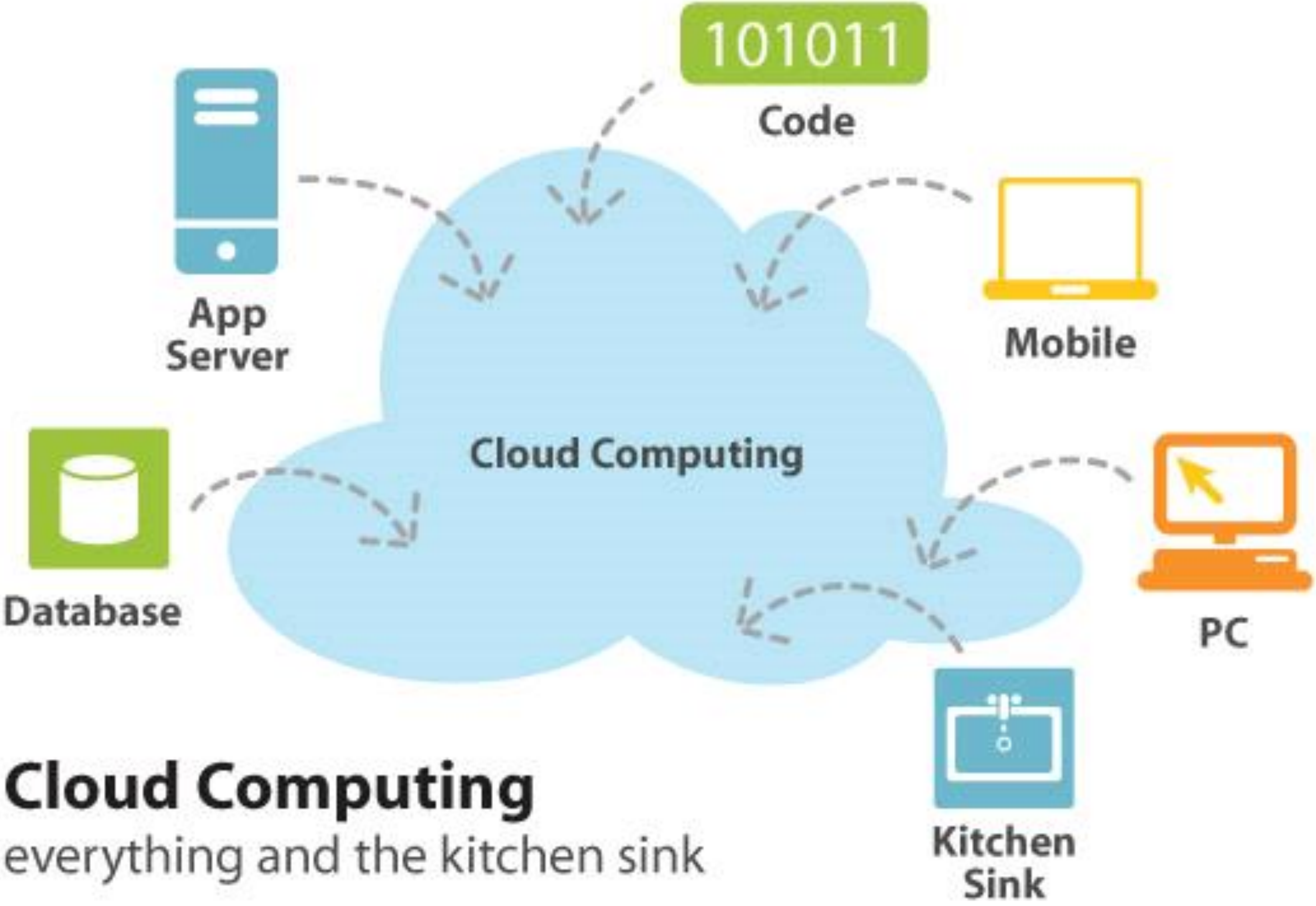
The Current Business Environment and Emerging Technology Risks

As highlighted in the previous slide, emerging technologies, while great for improving the effectiveness and efficiency of the business, also introduce risks.

Risk professional need to be able to understand these technologies in the context of the risk exposures they may create.

We will highlight a few of these technologies.

Emerging Technology Risks – The Cloud



Cloud Computing

everything and the kitchen sink

Emerging Technology Risks – The Cloud

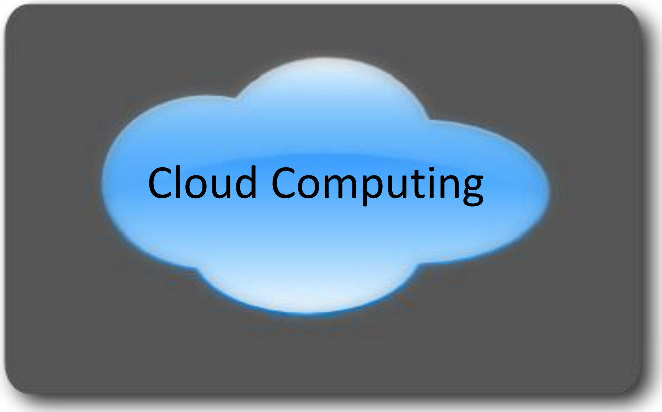
Definition

“Cloud Computing” is Internet-based computing, whereby shared resources, software, and information are provided to computers and other devices on demand, like the electricity grid.

Cloud computing, in theory, is the mass centralization of computing resources. Information, processing and software are then made available by tapping into this centralized cloud.

Cloud computing has the potential to be one of the largest revolutions in the history of the Information Technology (IT) industry. Benefits are many, but the potential to introduce risk is high unless risks are assessed and mitigated before moving into the cloud.

Emerging Technology Risks – The Cloud – 3 Models



Cloud Computing

Infrastructure as a Service

Platform as a Service

Software as a Service

Examples:

•Google Docs – Office productivity suite such as Calendar, Word Processing, Spreadsheet, E-mail (**Software as a Service**)

•Google's App Engine – offers the ability to code Web applications and then deploy and publish them in Google's cloud. (**Platform as a Service**)

•Amazon's Elastic Compute Cloud (EC2) service - allow users to create, customize, store and terminate computer servers, through virtualization, while paying for this service by the hour. (**Infrastructure as a service**)

Emerging Technology Risks – The Cloud

Benefits (e.g.)

- Allows extremely quick deployment of Infrastructure (e.g. servers).
- Very scalable.
- Low cost to distribute.
- Replaces high initial investment costs.
- Low computing resources on the user end – (e.g. may choose to use cheaper netbooks instead to notebooks and pc).
- Can be made available via different devices (e.g. smart phones / tablets).
- Central storage, simultaneous editing, offline editing.

Emerging Technology Risks – The Cloud

Risks

- Security and proper IT controls at service provider (3rd party risk).
- Governance (unapproved IT environments – staff may be running a business using company's technology).
- Bandwidth (capacity utilisation and speed).
- Data location in the cloud may change.
- Staff (lack of expertise may lead to errors, integrity etc.).

Emerging Technology Risks – Social Technologies

facebook®
twitter
g+
YouTube
Linkedin®
airbnb

Emerging Technology Risks – Social Technologies

Use in Business

- To promote business, products, service, events, etc. (e.g. Company Facebook, YouTube and Twitter pages).
- To send out general messages, news and other information to employees, customers and the public (e.g. Twitter).
- Conduct business - e.g. Take reservations (Open Table), sell movie tickets (Fandango, Flixter), rent apartment/home as a hotel (Airbnb).
- Open up a new channel for content delivery (e.g. News) at low cost, while making Ad revenue (YouTube).

Emerging Technology Risks – Social Technologies

Risks

- Increased SPAM to corporate email – where corporate email is used to register on these sites.
- Accounts compromises/hacks - to post inappropriate links or links that can be used for phishing attacks, or worse (steal customer and financial information).
- Increased risk to corporate network – e.g. from viruses embedded in user posts/links.
- Disclosure of confidential company information.
- Inappropriate communication to the world at large.
- Hackers or other unscrupulous persons can build a database of personal information to carry out attacks on said person or as said person (identify theft).

Social Technology Risk – An Example

First of all, sorry Dr. Langrin…

Many companies, in doing business with customers remotely (e.g. by phone or the Internet) ask customers to establish security questions and answers (e.g. Scotiabank customer care). However, in today's social era, this information can be easily attained by unscrupulous persons… and with a little **Social Engineering** know-how, they can get past these security checks…

I have never heard of, met or talked to Dr. Langrin until recently… However, I was able to obtain the following personal information on him, via the Internet in a few hours on the weekend…

YES, I do have a life!

Note – The information presented is "public". Not all information may be accurate.

Social Technology Risk – An Example

Name	Dr. Brian Langrin
Other Names	Ranse B Langrin
Education	Penn State University, Ph.D., Economics, 1996 – 2001
Age	42
Family info	Brian Langrin has a son Jacob and stepson Nathan Campbell, 12. He has a wife, Trudy Steer.
Father	Justice Ransford Langrin
Wife	Trudy (Steer) Langrin. Aquaworx Jamaica, Co-Founder Operator/Instructor, September 2008 – Present (5 years 7 months), @AquaWorx https://www.facebook.com/trudy.langrin Cell number - (876) 381-4123 Howard University Bachelor's degree in Psychology 1995 – 1999
Teaching Assistant for	Professor Barry W. Ickes, Spring 1999, for the course International Finance and Open Economy Macroeconomics, Economics 434, The Pennsylvania State University Department of Economics Office Hours: 3-4:30, Monday and Wednesday

Security Organization, User Awareness and Security Management

2011 13th Annual Sigma Corporate Run - 5K Run - Result	**47:18:00**
Twitter User Name	@langrin
Facebook Page	https://www.facebook.com/brian.langrin
Amazon Wish List	http://www.amazon.com/gp/registry/wishlist/3AK7QXA05AEZW
Flixter Profile Name	brianlangrin1
Flixter Top Movies - Rated 4 stars and above (in 2008)	Pirates of the Caribbean: The Curse of the Black Pearl - PG-13 Mr. & Mrs. Smith - PG-13 Charlie and the Chocolate Factory - PG Meet The Fockers - PG-13 The Lord of the Rings: The Return of the King - PG-13 Austin Powers in Goldmember- PG-13 Hitch - PG-13 Kill Bill: Volume 1 - R Braveheart - R The Matrix - R Gladiator - R There's Something About Mary- R

Social Technology Risk – An Example

I feel like I know Dr. Langrin now…

With almost everyone having a social presence, persons are key targets for criminal elements, who with a little time, can build a databases of information on persons to carry out social engineering and cyber attacks…

PwC has done this. For example, we were able to:

- Get account information (account number and balances) from customer care.
- Get personnel to initiate transactions remotely using fake emails of customers.
- Get passwords (from cold calls and email phishing) from employees, including senior personnel.
- Remove assets from office buildings (e.g. computers) using fake asset movement forms 'signed' by the CIO. The signature was found on the company's website.

Risk Professional’s Challenge

As risk professionals, we need to be able to identify and assess IT security risks within our organisations; and do this on an on-going basis.

Information technology (IT) security is one of the most frequently changing or evolving areas for risk professionals.

This requires continuous education, reading and research to keep up with changing, new and emerging technologies and the risks they present to the business.

This leaves us with the question… Where to begin with IT Security Risk…?

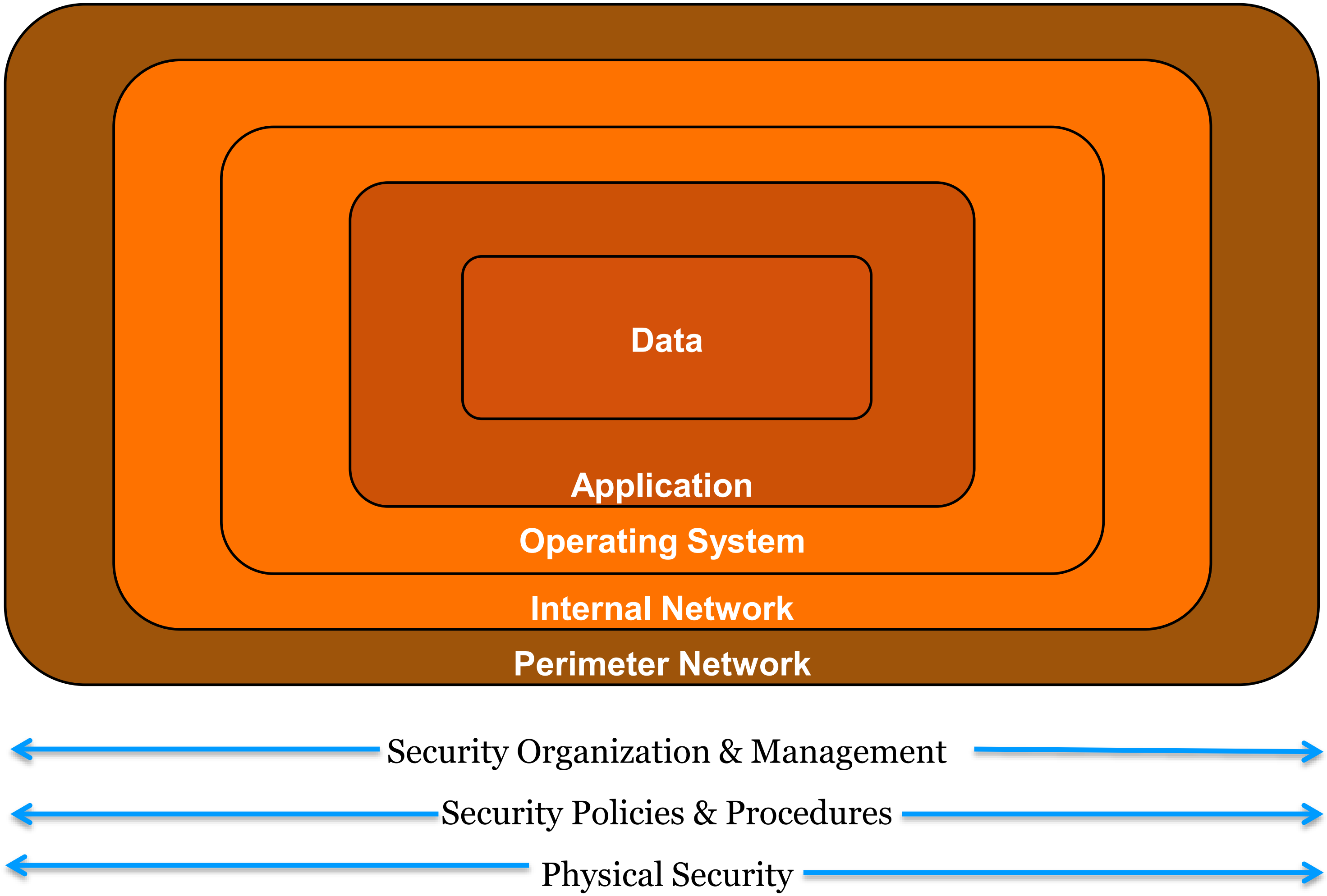
Information Security Risk – A Defense In-Depth Approach

In order to properly combat information security risks, no one solution can be applied. This is because information security is broad and varied. Management therefore has to adopt a ‘Defense In-Depth’ approach to tackle security risks.

This approach looks at information security in the following broad categories:

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- Data Security
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- Physical Security

Information Security Risk – A Defense In-Depth Approach



Information Security Risk – A Defense In-Depth Approach

- **Security Organization, User Awareness and Security Management**
- Security Policies and Procedures
- Security Administration
- Data Security
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- Physical Security

Security Organization, User Awareness and Security Management

- A member of the executive team should have ultimate responsibility for achieving the information security objectives of the organization.
- Information classification and handling procedures should be developed to guide how information assets are shared and protected.
- The functional security team should be designed to ensure an appropriate segregation of duties based on business requirements.
- Business unit management should “own” and approve all access to information/data.
- Security responsibilities should be formally documented and communicated.
- All employees should be periodically reminded / educated of their roles in achieving the organization’s information security objectives.
- Job applicants for sensitive positions should be subject to background checks, reference checks, etc.
- Changes in the technology landscape of the company, should be routinely assessed for security threats.

Security Organization, User Awareness and Security Management

This sets the tone for information security within, and even outside, the organisation.

The key is for **all stakeholders** to recognise that they are responsible for information security, and truly understand their roles and responsibilities.

It is not only the IT department’s responsibility to ensure information is secure.

IT can implement the strongest security mechanism, but security can be compromised in an instance, where users don’t understand their security roles and responsibilities.

Trust us, attackers look to use the people element to compromise security.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- **Security Policies and Procedures**
- Security Administration
- Data Security
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- Physical Security

Security Policies and Procedures

- Executive management has approved a complete set of information security policies and procedures that support the information security objectives of the organization.
- A process to change/update the security policies and procedures is defined and documented, and all changes/updates must be approved.
- The information security policies and procedures are readily available to all employees of the organization.
- IT and business users are all trained on information security policies and procedures when hired, and throughout employment.
- A process to ensure security policies and procedures are followed (i.e., monitoring) must be in place.

Overall Risk – Users may not be aware of their security roles and responsibilities, or security policies may be outdated as technology changes over time. This may result in execution of activities which may not sufficiently reduce the risk exposures to the business.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- **Security Administration**
- Data Security
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- Physical Security

Security Administration

Security Administration is the process for granting and removing access to information systems, data and resources. In other words, this is the process for:

- Granting users access to information systems, data and resources in accordance with their job responsibilities.
- Modifying users' access to the information systems, data and resources as changes occur (e.g. promotions).
- Removing users' access from information systems, data and resources where there is separation from the company.
- Periodically assessing users' access appropriateness to ensure that access remains commensurate with job responsibilities.
- Monitoring access to persons with elevated privileges.

Note - Users in the above context include, for example, employees, contractors, vendors and other stakeholders and third-parties.

Overall Risk – Users may have more access to systems, data and resources than necessary to carry out their job functions, which may result in them being able to circumvent controls and/or conceal unauthorized activities. In addition, where dormant accounts still remain on the system, this increases the risk of compromise to carry out unauthorised activities, which can no longer be associated with someone.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- **Data Security**
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- Physical Security

Data Security

Data is probably one of the most critical information assets of a business. It is the basis from which most financial and non-financial information is derived (for example, financial statements, business performance reports, customer statements, etc.). The criticality of data to a business is further exacerbated where no paper-trails/supports exist.

- Management should performs risk assessments over key databases and data.
- Management should implement controls to authenticate access to the database.
- Management should document and control who has access to view, modify and delete data.
- Where data needs to be changed, there must be a controlled process for doing so.
- Management should monitor access gained, and activities performed on data directly (e.g. view, update, delete, insert).

Overall risk – the integrity of the data and proper functioning of the system may be jeopardized where inappropriate access is granted or gained. In addition, confidential (e.g. customer credit card information) and restricted (e.g. company's market strategy) information may be compromised, which may have far reaching effects.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- Data Security
- **Operating System Security**
- Internal Network Security
- Perimeter Network Security
- Physical Security

Operating System Security

The Operating System is the software environment on which all applications, databases and hardware components communicate in an interactive way. Think of the operating system as your body, which along with your the brain, organs and muscles, makes everything work. Examples of operating systems include Windows 7, Unix, Android, iOS.

- Management should assess the risk over the operating system environment (e.g. Servers, notebooks, mobile devices, etc.).
- Management should implement controls to authenticate access to the operating system (e.g. your network user name and password).
- Only authorized personnel should have the ability to make changes to security and other settings.
- Management should document and control who has access to and within the operating system environment (e.g. only IT personnel has access to servers or user should not have the ability to install programs).
- Management should monitor access gained to, activities performed and changes within the operating system environment.
- Automated security software (e.g. anti-virus programs) should be implemented.

Overall risk - the integrity of the programs, data and proper functioning of the system may be jeopardized where inappropriate access is granted or gained. Unauthorized access may also be used to launch attacks on other systems and networks.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- Data Security
- Operating System Security
- **Internal Network Security**
- Perimeter Network Security
- Physical Security

Internal Network Security

Think of your internal network as your house, which contains all rooms, their content (systems, data and resources) and your family (users). This is your private sanctuary (business) where you conduct your personal (business) matters. Your internal network therefore contains all the hardware and software components to connect all your users, computers, and other devices together to conduct business.

Similar to your home, businesses need to implement sufficient controls to protect the internal network. For example:

- Implement intrusion prevention or detection controls (e.g. your home alarm, motion sensors, security cameras).
- Segment users from servers, and implement access controls to allow/deny access (e.g. door locks on rooms for mommy/daddy vs. kids, parental control software on tvs and computers).
- Limiting who can access and administer the network (e.g. only parents can arm and disarm the alarm, and call off the security).
- Monitor for security related events and activities (e.g. peek-through windows for kids rooms, nanny or parents periodically checking on the kids, monitoring software on tvs and computers).

Overall Risk – Unauthorised persons may gain access to the systems and resources (all the rooms and content), or prevent users from carrying out their activities (prevent parents from calling the security or exiting the home).

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- Data Security
- Operating System Security
- Internal Network Security
- **Perimeter Network Security**
- Physical Security

Perimeter Network Security

Think of your perimeter network as your gate/fence around your home or apartment complex. This gate/fencing prevents unwanted persons from entering, while also allowing those authorised persons to come in and go out.

Your perimeter network protects your internal network (house/apartment) from external networks, for example the Internet. You would not want just anyone to be able to stroll in and out from the road? When someone breaches your fence/gate, this is similar to an hacker getting into your network.

Businesses need to implement sufficient controls to strengthen their perimeter network. For example:

- Implement a firewall (e.g. a gate with a security guard) which has access list for what is allowed in and out (e.g. guest list used by the guard).
- Implement security filters to block as much unauthorised traffic as possible (e.g. a sign that says “Protected by Guardsman”).
- Limiting who can access and administer the perimeter network.
- Monitoring for security related events and activities (e.g. checking the guard access log, security cameras, etc).

Overall Risk – Unauthorised persons may gain access to the systems and resources, or prevent users from carrying out their activities through a denial of service attack.

Information Security Risk – A Defense In-Depth Approach

- Security Organization, User Awareness and Security Management
- Security Policies and Procedures
- Security Administration
- Data Security
- Operating System Security
- Internal Network Security
- Perimeter Network Security
- **Physical Security**

Physical Security

Just as the other security layers, physical security is of paramount importance. This also has to be combined with user security awareness to be fully effective.

Physical security is also one of the main ways an attacker will try to access a business, and then use social engineering techniques to get access to assets and information. PwC has performed several of physical security reviews, where we have been able to:

- Access the buildings and offices, bypassing security guards and staff, through vulnerable access doors.
- Collect assets and documents from offices and from trash bins. Some of the information in the trash bins contained sensitive information.
- Shadow employees to gain access to locked areas.
- Get users to logon to their computers for us to access their data and applications.

Some physical security measure businesses should consider include:

- Protecting buildings/sites using a card key access system, particularly sensitive areas.
- Implementing a formal security administration process to grant, change and remove access.
- Educating staff and contractors on security procedures (e.g. visitor escort, shadowing, visitor challenging, clear screen/clear desk, document disposal, etc.)

Summary

As risk professionals, we can use this defense in-depth approach to have discussions with the various IT and business stakeholders, to understand the security risks and controls in place from a modular standpoint. This approach alongside reading, research and, in stances, some technical assistance can equip you to build your IT security risk universe and audit plan…

Risk professionals can no longer be intimidated by Information Technology. I have always said, you don't have to be a full techie to audit, you have to understand **risk and controls**.

We are here to assist you where the need arises…

Creating a culture of
risk awareness™

**Global Association of
Risk Professionals**

111 Town Square Place
Suite 1215
Jersey City, New Jersey 07310
USA
+ 1 201.719.7210

2nd Floor
Bengal Wing
9A Devonshire Square
London, EC2M 4YN
UK
+ 44 (0) 20 7397 9630

www.garp.org

THANK YOU

About GARP | *The Global Association of Risk Professionals (GARP) is a not-for-profit global membership organization dedicated to preparing professionals and organizations to make better informed risk decisions. Membership represents over 150,000 risk management practitioners and researchers from banks, investment management firms, government agencies, academic institutions, and corporations from more than 195 countries and territories. GARP administers the Financial Risk Manager (FRM®) and the Energy Risk Professional (ERP®) exams; certifications recognized by risk professionals worldwide. GARP also helps advance the role of risk management via comprehensive professional education and training for professionals of all levels. www.garp.org.*

GARP | Global Association of Risk Professionals