MOORE STEPHENS

THE INSTITUTE OF INTERNAL AUDITORS
IIA INTERNATIONAL CONFERENCE
DUBAI, UAE / 6-9 MAY 2018

DUBAI2018

Information Security

Protecting Privacy

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Unless otherwise stated copyright in the hole and every part of the information belongs to Moore Stephens LLP, and may not be used sold, licensed, copied or reproduced in whole or in part in any manner or form or in any media to any person without written consent. Although care has been taken to ensure the content is accurate and timely, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future.

Moore Stephens LLP therefore accepts no liability for loss of any kind incurred as a result of reliance on the information or opinions provided in this presentation. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

Introduction

Anthony Blenkey

AGENDA

- Information Security Regulatory Developments
- Advancing Internal Audit’s role and function in identifying information security risks;
- Management Compliance with International Information Security Requirements
  - techniques to assess information security issues; and
- Internal Audits Role in Information Security Breach Detection.

Current Developments in Information Security Regulation – Maintaining Privacy

DEFINITIONS – WHAT ARE WE TALKING ABOUT?

Information Security: In part, refers to the control of information and data risks associated with the business. The way in which information and systems are protected from unauthorised change, access, damage , disruption, or release.

Information security is a **set of strategies** for managing the processes, tools and policies necessary to **prevent, detect, document and counter threats to digital and non-digital information.** Information security responsibilities include establishing a set of business processes that will protect information assets *(Source – TechTarget Essentials, A Guide for CIOs)*

Data Privacy: or information privacy, concerns the collection, **protection and dissemination** of personal or private information about individuals or organisations.
(Source – Financial Times Lexicon)

Personal Data: means data which relate to a living individual **who can be identified** –
(a) from those data, or
(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the **data controller**, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual. *(Source - UK Information Commissioner's Office)*

Current Developments in Information Security Regulation – Maintaining Privacy

Examples of Key International Legislation and Regulation:

USA: Federal Information Security and Management Act (FISMA) enacted in **December 2002** as part of the E-Government Act of 2002.
Cybersecurity Enhancement Act of **2014 –** *(NIST Risk Framework).*
Cybersecurity Information Sharing Act (CISA) passed in the Senate **October 2015**.
Federal Exchange Data Breach Notification Act of **2015**.

UK: Coming This Month - General Data Protection Regulation (GDPR - effective 25th May 2018) – Includes Europe.
Malicious Communications Act **1988**
Computer Misuse Act **1990**
Data Protection Act **1998**
Freedom of Information Act **2000**
Privacy and Electronic Communications Regulations **2003**
Digital Economy Act **2010**

Canada: The Digital Privacy Act **2015**
Federal Personal Information Protection and Electronic Documents Act **2000 - (PIPEDA)**
Alberta's Personal Information Protection Act **2003**
British Columbia's Personal Information Protection Act **2003**
Québec's An Act Respecting the Protection of Personal Information in the Private Sector
Telecommunications Act **2010**

Current Developments in Information Security Regulation – Maintaining Privacy

Examples of Key International Legislation and Regulation:

Australia: Telecommunications (Interception and Access) Act **1979**
Privacy Act **1988 -** Australian Privacy Principles (APP)
Cybercrime Act **2001**
Spam Act **2003**

UAE: Federal Law No. 3 of **1987** concerning the Penal Code Regulating Telecommunications (Federal Law by Decree 3 of **2003** as amended).
NESA – Federal Law No. (7) of **2002**: Intellectual Property.
Federal Law No. (1) of **2006**: Electronic Commerce and Transactions.
Federal Law No. 5 of **2012** (as amended by Federal Law No. **12/2016)** Combating Information Technology Crimes (the Cybercrimes Law).

China: Cyber Security Law (the ***CS Law***), came into effect June **2017**
Final version of the national standard on personal information protection – **May 2018**

Russia: Federal Law on Personal Data (No. 152-FZ), implemented on July **2006**
Information Act (Federal Law 149-FZ), July **2006**.

Current Developments in Information Security Regulation – Maintaining Privacy

CYBER CRIME - The Case For More Privacy Legislation and Security of Personal Information.

CASE STUDIES:

- **Facebook & Cambridge Analytica** - Data leak hits 87 million users, widening privacy scandal (Source: Reuters April 4th 2018);
- **UK Information Commissioners Office (ICO):** *UK's independent authority set up to uphold information rights* - **Hackers hijack government websites to mine crypto-cash** (Source: BBC News Feb 18th 2018);
- ***MyFitnessPal*** application - Hackers steal data of 150 million users. The breach occurred in February and was reported in March. (Source The Guardian 30th March 2018); and
- **Fedex** - Thousands of customers' private information exposed in legacy server data breach (Source: The Inquirer 16th Feb 2018).

Current Developments in Information Security Regulation – Maintaining Privacy

The Facebook and Cambridge Analytica scandal teaches us how little most people understand about data brokering, adtech and digital marketing industry operations and the associated information security risks.

The IAB Data Centre of Excellence and the Data & Marketing Association (DMA) released "**The State of Data 2017**," a study showing that U.S. companies alone will have spent **$10.05 billion** on third-party data in 2017.

1st Party Data – Your company's data which is taken from the data source (usually a data subject who has agreed to provide information for processing);

2nd Party Data – Another company's data which may have been purchased directly from them or be exchanged within a business group i.e. comes from the source data controller.

3rd Party Data *– Amalgamated from numerous sources and bought and sold on data exchanges etc.*

Current Developments in Information Security Regulation – Maintaining Privacy

Increased Use and Reliance on IT and Personal Data Collection over the last 10 years The Case For More Privacy Legislation and Security of Personal Information.

Technological Advancement:

- **Smart Phones –** The latest iPhone X and Samsung S9 mobile phones have more data storage and processing power than most laptops had 10 years ago.
- **Smart Watches** – Fitness applications, messaging on the go. Ubiquitous use of these types of devices didn't exist 10 years ago.
- **Smart Home Appliances** – Televisions, Fridges, Lights, Door Bells are all busy gathering your information and processing it to deliver personalised services.
- **Digital Assistants or AI** - Amazon Echo, Google Home, Siri, Cortana.
- **Satellite Navigation -** GPS & Geotag devices and applications know where you are and the journeys you take and where you've been.

A personal information data frenzy is currently taking place and large numbers of 'data subjects' are not paying attention.

Current Developments in Information Security Regulation – Maintaining Privacy

Different Generations have widely differing views on Personal Data Privacy.
Some may need protecting from themselves:
The demographic of the workplace has changed significantly over the last 30 Years. **In the coming two to three years it is expected that for the first time - 5 Generations** may be in the workplace simultaneously. This is Comprised of the:

- **Traditionalists** (born after 1946);
- **Baby Boomers** (born 1950 -1964);
- **Generation X / Busters** (born 1965-1980);
- **Generation Y / Millennials** (born 1981-1994); and
- **Generation Z / Digital Natives** (born after 1994).

The different behaviours and approaches displayed by each demographic in respect of IT and Data Security can equate to a BIG RISK

Current Developments in Information Security Regulation – Maintaining Privacy

General Data Protection Regulation (GDPR - Effective 25th May 2018)

WHAT IS IT and WHY SHOULD INTERNAL AUDITORS CARE?

- It's a piece of **EU legislation** which aims to create duplicate or equal data privacy laws across the **whole of the EU**.
- **The legislation is far reaching** and encompasses **all EU 'data subjects'** and their personal information i.e. **Territorial scope increased to a global level:** If you process data of subjects residing in the EU **you will have to comply** with GDPR even if your company is located elsewhere;
- **Big financial penalties** for abuse or breach – punitive fines: up to **€20 million** or **4% of your global annual turnover.** Fines can apply to both Data Controllers and Data Processors;
- **Large scale reputational damage** and potentially the ability to continue as a 'going-concern' due to public loss of confidence.

Current Developments in Information Security Regulation – Maintaining Privacy

General Data Protection Regulation (GDPR) - Other Regulatory Requirements:

- **Privacy By Design and Privacy Impact Assessments;**
- **Right To Be Forgotten -** Erasure**;**
- **Right to Access and Portability of personal data;**
- **Data Protection Officer (DPO) – new requirement;**
- **If Information Systems Breached** – 72 Hours to Report (*From time of identification*);
- **Classify 'Personal Information'** in terms of risk. In addition, know which legal basis the data your business is applying to different types of information;
- Require a level of **proof** that active steps to ensure compliance with the GDPR Regulations; and
- **Active and Affirmative Consent** (where required). No more passive 'opt-in'.

Current Developments in Information Security Regulation – Maintaining Privacy

General Data Protection Regulation (GDPR)

This time last year ‘Gartner’ predicted that **by the end of 2018, more than 50% of companies affected by the European General Data Protection Regulation (GDPR) will not be in full compliance with its requirements.**

- Lack of awareness or understanding of Cross-Border data flows;
- Insufficient preparation in anticipation of ‘Data Subjects’ utilising their new rights (or lobby groups); and
- Not understanding the global implication of GDPR in relation to ‘EU Data Subjects’.

Internal Audit’s Role and Function in Identifying Information Security Risks

International Professional Practices Framework and the Internal Audit Standards Key Relevant Requirements:

- **IIA Standard 2110 A2** - The internal audit activity **must assess whether the information technology governance** of the organisation supports the organisation's strategies and objectives.

- **IIA Standard 2120** - The internal audit activity must evaluate the effectiveness and contribute to the improvement of **risk management** processes.

- **IIA Standard 2130** - The internal audit activity must assist the organisation in **maintaining effective control**s by evaluating their effectiveness and efficiency and by promoting continuous improvement.

Internal Audit’s Role and Function in Identifying Information Security Risks

Why are Information Security Risks An Important Issue For Internal Auditors To Tackle?

The Cyber Crime Issues Facing Businesses of All Sizes

‘Forbes’ recently indicated that from 2013 to 2015 the cyber crime costs **quadrupled,** and it looks like there may be another quadrupling **from 2015 to 2019**. ’Juniper Research’ recently predicted that the **rapid digitization of consumers’ lives** and enterprise records will increase the **cost of data breaches to $21 trillion globally by 2019**, increasing to almost four times the estimated cost of breaches in 2015.

Large banks, retailers, and government bodies make the headlines when they are hacked - but all businesses are at risk. **According to ‘Microsoft’** - **20% of small to medium sized businesses have been cyber crime targets.**

Internal Audit's Role and Function in Identifying Information Security Risks

Knowing what your Company's information security risks are and where in their systems the material risks reside, is an area where Internal Audit can have significant impact.

Undertake An Information Mapping Assessment Across The Business

Internal Audit function will routinely assess risks associated with:

- **Processes;**
- **Policies;**
- **People;**
- **Infrastructure;**
- **Hardware; and**
- **Software.**

The first step for Internal Audit to identify risks is to establish a clear baseline. **Developing a complete picture** of all information assets held and confirming ownership, accountability and responsibility.

Internal Audit's Role and Function in Identifying Information Security Risks

Information Security Risks – Internal Audit Continuous Monitoring:

- **Mobility and Globalisation – Communication and security risks can travel.**

  People are now connected and working:

  - **At Any time (across time zones);**
  - **Any Place (location no longer matters); and**
  - **Any Device**

  Work can be taken with you wherever you and this means the Information and Privacy Risks can grow exponentially. Increased risk that devices are lost, stolen or compromised. Information is released by accident due to tired staff mixing up personal and work Twitter or Facebook accounts etc.

- **A forward focus and the use of AI can help Internal Audit functions direct their resources to identify issues and support management in mitigating risks.**

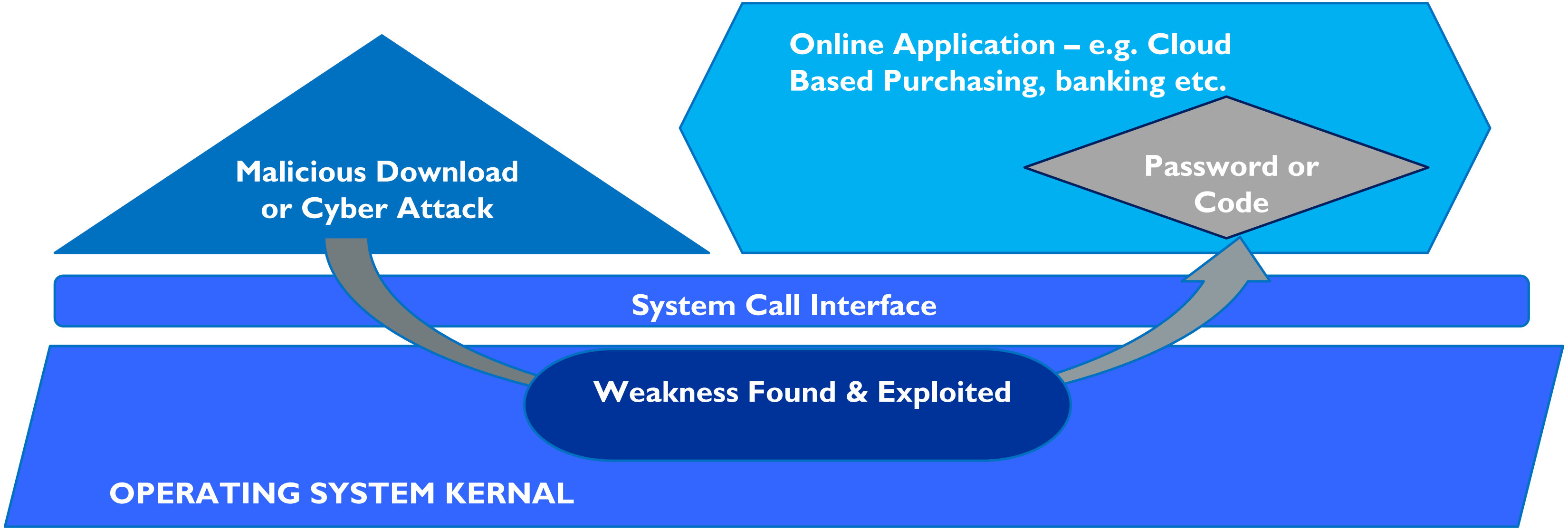
Internal Audit’s Role and Function in Identifying Information Security Risks

Top Cyber Threats (Source: Computer Weekly 2016 and Wired)

- **Ransomware** – some studies indicate that as many as 1 in 5 businesses affected by ransomeware are forced to close. **Wannacry** spread around the globe and impacted hundreds of thousands of targets. Wannacry was followed closely by the release of **Petya, NotPetya** and a few other names, this was more advanced than Wannacry;
- **Distributed Denial of Service** – Cyber act of vandalism, disrupting businesses or extorting money from businesses;
- **Hacking** – e.g. **3. 412 million user accounts exposed** in **FriendFinder** Networks hack, Bank accounts (Tesco 2.5million) hacked;
- **Cloud-Bleed** – Data Leakage;
- **Industrialised Cyber Crime** – Professional cyber criminals who target a business and then utilise freely available employee information to access systems (**Facebook, Twitter, LinkedIn etc.**); and
- **Phishing and Spear Phishing** – Use of well known companies as camouflage for obtaining confidential information or using links which then allow access to your systems.

Internal Audit's Role and Function in Identifying Information Security Risks

Managing Information Security Threats from the Bottom Up


Online Application – e.g. Cloud Based Purchasing, banking etc.
Malicious Download or Cyber Attack
Password or Code
System Call Interface
Weakness Found & Exploited
OPERATING SYSTEM KERNAL

Internal Audit’s Role and Function in Identifying Information Security Risks

Leveraging Big Data to Assess Information Risk Across the Business

Big Data and Artificial Intelligence and be utilised by Internal Audit to drill down and assess cyber risks - Lloyd’s of London report “**counterfactual risk analysis**”, outlines a technique that involves imagining in detail how the past might have turned out differently to inform better risk modelling for businesses. Broader movement in risk analysis towards using **big data, artificial intelligence** and fresh approaches that should help yield vast improvements in forecasting.

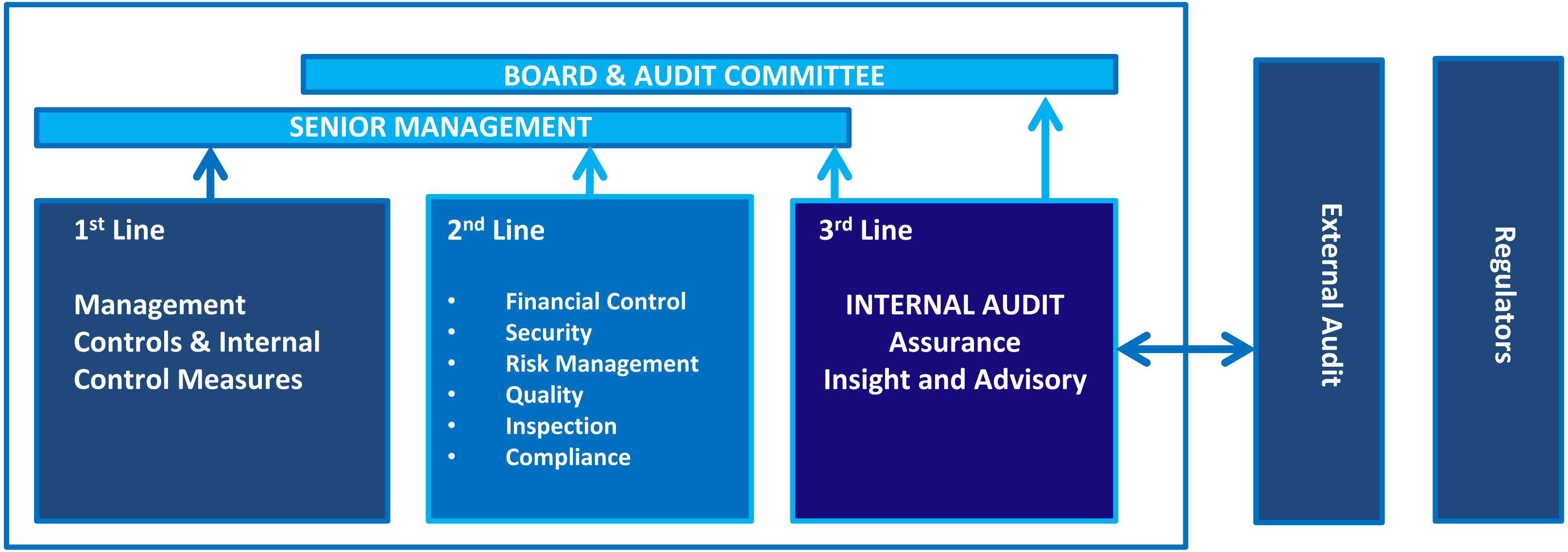
Improved predictions should lead to a lower frequency of extreme events and/or less severity when they occur. Better resilience and preparedness will mean information security breach impacts are reduced and costs minimised.

Improved technology, data analytics and artificial intelligence mean that **events that occurred at the margins of a normal pattern or distribution can now be added into the mix to generate a more realistic model** and allow better scenario analysis. However, this type of technology requires investment.

Are your investing?

Internal Audit's Role and Function in Identifying Information Security Risks

Internal Audit Leveraging the Three Lines of Defence Model to Improve Information Security Risk Management as Independent Assurance Providers



BOARD & AUDIT COMMITTEE

SENIOR MANAGEMENT

1st Line

Management Controls & Internal Control Measures

2nd Line

- Financial Control
- Security
- Risk Management
- Quality
- Inspection
- Compliance

3rd Line

INTERNAL AUDIT
Assurance
Insight and Advisory

External Audit

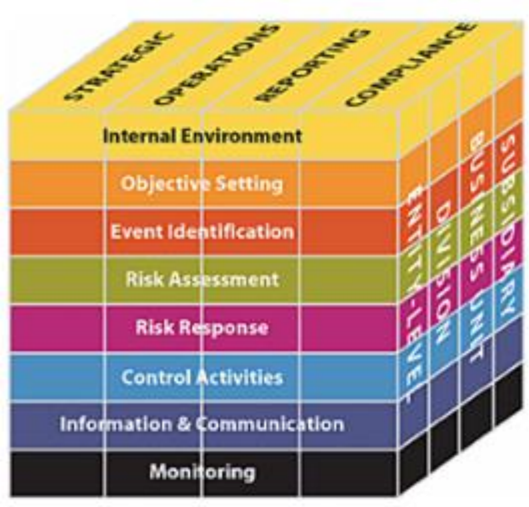
Regulators

MOORE STEPHENS

THE INSTITUTE OF INTERNAL AUDITORS INTERNATIONAL CONFERENCE
DUBAI, UAE / 6-9 MAY 2018
DUBAI 2018

Internal Audit's Role and Function in Identifying Information Security Risks

Adding Value



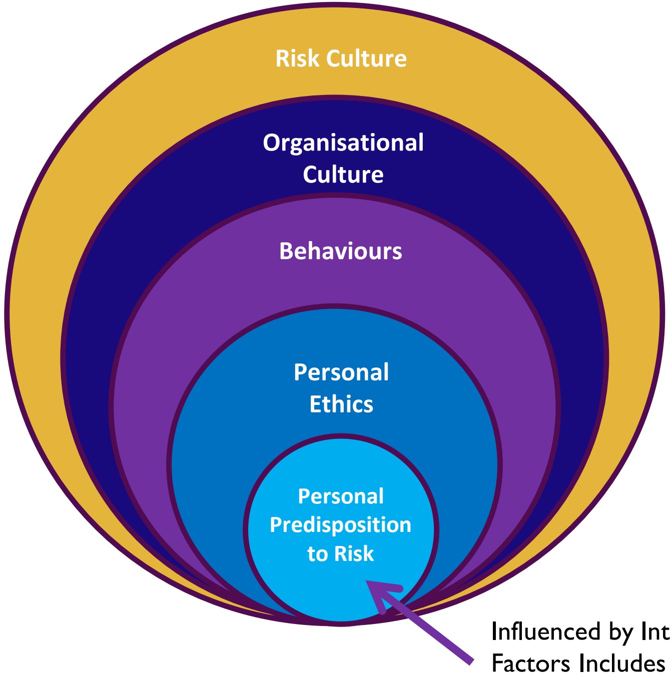
Committee of Sponsoring Organizations of the Treadway Commission (COSO) ERM Framework

- Seek to utilise the **8 components of the COSO ERM Framework** to help management balance cost and benefit when undertaking an assessment of the differing Information Security Risks across the range of business functions and activities. Use the matrix to manage the drill-down to business unit and subsidiaries.

- Support operational performance with assurance and recommendations to generate process efficiencies and produce cost effective controls. Look to '**Predictive Analytics**' to assess the potential and possible severity of internal and external factors. **Know the norms** and utilise them to help the business protect, detect and deter.

Internal Audit's Role and Function in Identifying Information Security Risks

Information Risk Awareness, Behaviours and Culture Interrelationships (IRM)



Influenced by Internal and External Factors Includes Generation (Cyber History and Social Norms)

The **Institute of Risk Management (IRM)** has developed a Risk Culture Framework. Their Diagram helps to demonstrate the complex interdependent set of relationships between personal risk awareness, behaviours and the wider organisational culture and overarching Risk Culture. This can be overlaid on the Culture of the business.

An organisation's Risk maturity and Culture is a crucial factor in setting behavioural standards. By looking at **Information Risk Maturity,** Internal Audit can give the Board a realistic picture of how well information risks across the organisation are being managed and how effectively privacy risks are being considered and mitigated.

Management Compliance with International Information Security Requirements

Why is Internal Audit Helping Management with Information Security So Important?

Gemalto Statistics – Data Breach Level Index

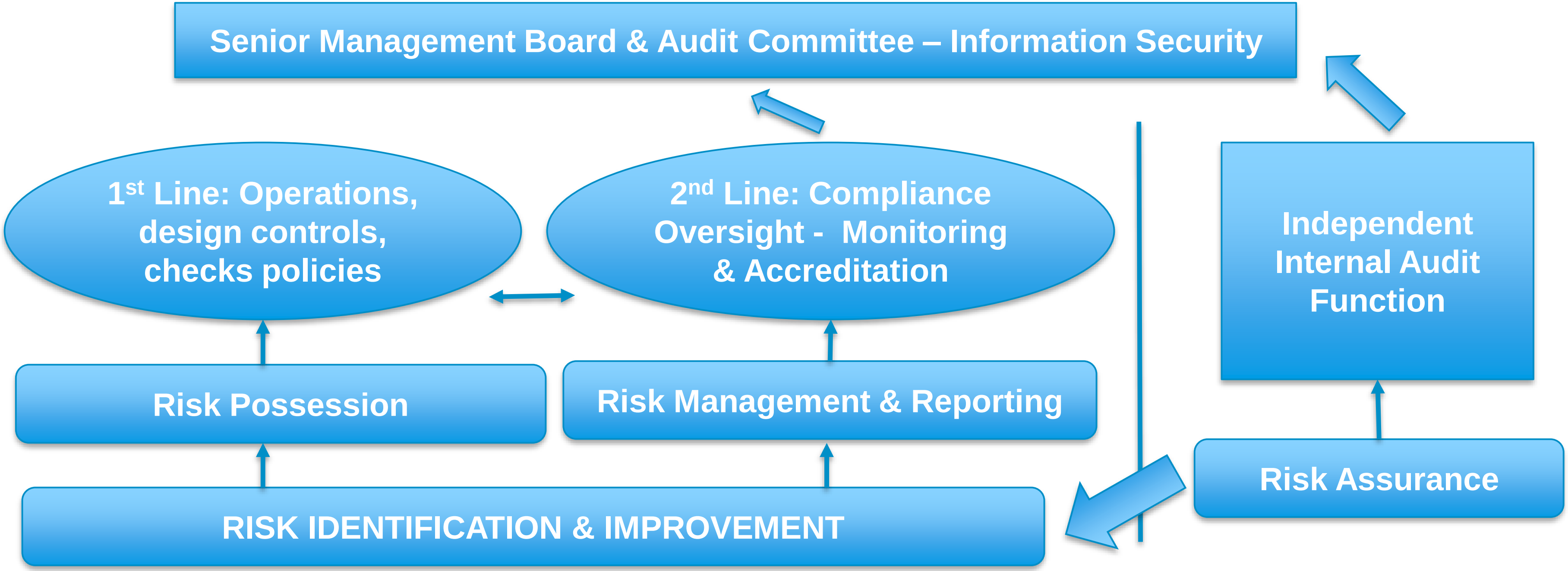
Break down of the 2017 Breach Level Index statistics:

- **7,125,940** compromised every day
- **2,96914** compromised records every hour
- **4,949** compromised records every minute
- **82** compromised records every second

According to the new Breach Level Index (BLI), in 2017, the number of data records compromised in publicly disclosed data breaches surpassed **2.5 billion, up 88% from 2016.**

Management Compliance with International Information Security Requirements

Three Lines of Defence – Lines 1 and 2



Senior Management Board & Audit Committee – Information Security

1st Line: Operations, design controls, checks policies

2nd Line: Compliance Oversight - Monitoring & Accreditation

Independent Internal Audit Function

Risk Possession

Risk Management & Reporting

Risk Assurance

RISK IDENTIFICATION & IMPROVEMENT

Management Compliance with International Information Security Requirements

Three Lines of Defence – Line 1 (applies to Operational Managers and employees): Key Areas

- Development of policies and processes to maintain **secure device, infrastructure and network security configuration**;
- Develop and deliver **training, testing** and appropriate information security **procedures**;
- Position data protection and **data intrusion detection** systems and applications;
- **Map all data flows and sources, Map all cyber assets**;
- Maintain a **full list of systems, access rights and privilege** roles;
- Maintain the capability to **encrypt certain types of data**;
- **Apply vulnerability testing** and demonstrate timely response to any issues raised; and
- Apply **business continuity and disaster recovery** procedures.

Management Compliance with International Information Security Requirements

Three Lines of Defence – (Senior Managers and Compliance) - Line 2: Key Areas

- Undertake regular and periodic **information security and data privacy risk assessments;**
- Collect and compile **information security threat intelligence** and known **attack patterns;**
- Develop **information security and data privacy policies**, supported by training and awareness;
- Lead in **classifying data and information types** to ensure the correct level of protection is afforded (may require specialist input);
- Undertake regular and periodic assessment of **3rd Party information security and data processing risks and relationships**; and
- Confirm by testing, the adequacy of **business continuity and disaster recovery**.

Management Compliance with International Information Security Requirements

To support 'leading practice' and regulatory compliance management should look to - Frameworks and Governance:

- **ISO 27001** – Information security management system standard. The 27000 series is a number of standards which help support businesses in securing information assets;
- **COBIT 5** – A framework for the governance and management of enterprise IT
- **NIST Cyber Security Framework** – National Institute of Standards and Technology (U.S Department of Commerce.

Perhaps one of the most helpful frameworks for both management and Internal Audit is NIST Cyber Security Framework. There is read-across to the ISO standards and COBIT 5. By using these standards and frameworks both management and Internal Audit can effectively assess the end to end approach to information security and form an holistic opinion.

NIST Cyber Security Framework has 5 key areas for development and control. These are:

- **Identify; Protect; Detect; Respond; Recover.**

Management Compliance with International Information Security Requirements

The Threat Landscape

Large numbers of people are now more comfortable sharing their personal lives and thoughts online.

- **Blogs** - Professional & Personal Information;
- **Twitter** – Professional and Personal Information;
- **Facebook** – Personal Information;
- **Instagram** – Personal Information;
- **Snapchat** – Personal Information;
- **LinkedIn** – Professional Information;
- **WhatsApp** – Professional and Personal Information;
- **Yammer;** and
- **Rate My Service sites** (Hotels, Plumbers, Amazon etc…)

This provides a wealth of data and information that can be leveraged by individuals or organised crime rings that indulge in:

- **Hacking;**
- **Phishing and**
- **Loading and activating Malware.**

Management Compliance with International Information Security Requirements

Supporting management's role: Internal Audit Validation of Data – Key Questions?

- Does the management within your business have the ability to adequately challenge and assess the information, business plans, KPI dashboards they are being presented with?
- Do they have the skills to look behind the data or information a which has been provided. Are they aware of dark data?

Internal Audit can help by offering to assess and analyse data which has been used to provide information to senior management and the Board.

Management Compliance with International Information Security Requirements

In conjunction with management Internal Audit should also be confirming if the business has a Data Security Action plan (or similar).

- **When was it last reviewed?**
- **Does it effectively cover all IT assets (systems, devices including BOYD etc.)?**
- **When was it last tested – Does everyone know what to do if or when a cyber event occurs?**

All of the above questions help support management in developing the accurate level of insight required to make the most informed decisions about information security.

Management Compliance with International Information Security Requirements

Internal Audit can support management to underpin information security regulatory compliance:

- **Facilitate consideration of what information is deemed critical and why** – If employees understand the significance of the data they use and the applications they operate there is a better chance they will be able to deal with the threats appropriately.
- **Help raise awareness of the value of the data and IT Assets** they use (to fraudsters, competitors, etc.)
- **Confirm that management know exactly where the information they use is held and how it is accessed.** This can then be mapped to where it is processed, and stored and any specific vulnerabilities assessed.
- **Confirm that management have fully established how employees and 3rd Parties use data** and how the information is transmitted. Again, an assessment should be made of potential information and privacy vulnerabilities (of particular relevance RE: GDPR).

Management Compliance with International Information Security Requirements

Internal Auditors supporting management in answering the question:
Is the Wi-Fi employees use always secure? (A question that should be continually re-visited)

- Do operational systems highlight or lock out unsafe connections and sites effectively? Some staff will be 'Cyber Savy' but others will be less prepared. **Internal Audit can see if the controls are in place or test those that are to see whether they are working effectively.**
- Do all your staff across the business understand the IT risks when travelling or using IT outside of the office network and are they aware of how to treat them? **Internal Auditors are well placed to consider the effectiveness of training and awareness.**
- Are employees functioning as individuals with access and awareness to the technology of the moment whilst your business operates a decade behind? **Is BOYD being applied regardless of business policy or in the absence of a policy?**

Internal Audits Role in Information Security Breach Detection

Internal Audit Providing Insight

A **disgruntled, disaffected or desperate** employee can cause more damage than an external cyber attack. Perpetrators generally have more time to gather the data they want and have a better idea where to find it.

The well publicised **US National Security Agency (NSA) Data Breach of 2013 by Edward Snowden** is probably the best example of what can happen when trusted insiders have widespread and uncontrolled access to the organisation's data.

Internal Audits Role in Information Security Breach Detection

Internal Audit should take time to look at staff profiles and can request to be informed when staff with sensitive data privileges indicate a desire to leave the business or resign. Early monitoring and assessment of activity can help prevent an internal data or privacy breach. **Understanding the risk profile of employees** can help businesses better manage information security risks and the threat from cyber fraud.

Practical measures include - continuous audit controls (Red Flags):

- Regular monitoring and alerts in respect of **unauthorised internal access or attempts**;
- Notification or discovery of the **violation of organisation policies**;
- Internal reconnaissance – **assessing the mood** in the business and considering sensitivities;
- Looking more closely at **instances of 'Data loss'** – Was the loss accidental, deliberate or malicious?
- Looking for staff who may be '**Data Hoarding**'.

Internal Audits Role in Information Security Breach Detection

Confirm whether:

- IT Management regularly assess and review the categorisation and protection levels of business information and how easy it would be for unauthorised access to occur.

  The **technological ability of hackers and organised criminals is continually improving and they are currently focusing on the weakest link in the chain which is likely to be your employees.**
- Cyber resilience testing performed (penetration, vulnerability, access, tracking changes, configuration management etc.)
- Consider how is cybersecurity risks are monitored for those who have **functional access to critical information**?

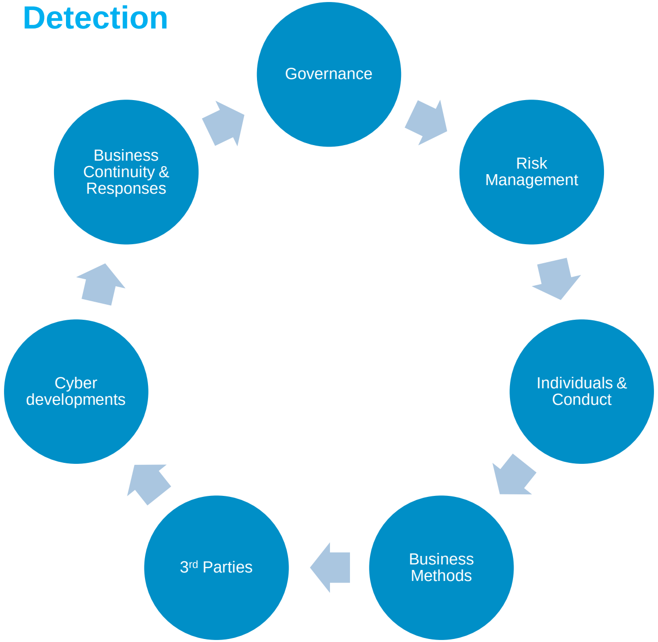
Internal Audit can play a key role in anticipating future risks in relation to security risks through the creation and maintenance of "watch lists", ensuring that certain risks, roles and sector specific threats are identified and prepared for.

Internal Audits Role in Information Security Breach Detection

The Elements of Breach Detection are Multifaceted:

- Detection of a breach is **not the sole responsibility of the IT Department.** Internal Audit has a vital role to play.
- The testing undertaken by Internal Auditors and unique position within the business **allows a mix of techniques to be applied.**
- Well trained and qualified Internal Audit staff are essential. They are the ones who can identify the **'root cause' of the issue**. Investment is vital.
- As demonstrated from earlier slides, the statistics in respect of data breach demonstrate it is a very real and active risk **requiring proactive monitoring**.
- Knowing the r**elevant local and international regulations.** To support the business internal auditors must understand what the compliance parameters are.

Elements of Breach Detection



Internal Audits Role in Information Security Breach Detection

Internal Audit and Root Cause Analysis and Data Breach

There are 5 Critical Areas where Internal Audit needs to look after a data breach has occurred in order to get to the **‘Root Cause’** of the issues:

- Governance;
- Processes;
- Security Training and Awareness;
- Data Mapping and Privacy Impact Analysis;
- People and Communication (Who, What, Why, Where, How and When).

There are other areas where symptoms of poor or inadequate information/data Security control may manifest but in the majority of cases the underlying root of the problem will usually come back to one of the above 5 categories.

Internal Audits Role in Information Security Breach Detection

Cyber Security Tools - Breach Detection Software:

The focus has been on the internal threat as they are already inside your firewall. External threats also exist. One of the most straightforward ways to identify both sources of data breach is via **‘Detection Software’** (may be referred to as ‘Active Threat Detection’).

Modern and breach detection systems now:

- Utilise complex algorithms and analytical tests to seek out potential information breaches. Algorithms can assess expected behaviours in relation to new behaviours or alert staff to abnormalities from standard patterns.
- To some extent can perform a low-level AI role.
- Go beyond rule based methods and if selected correctly can be a robust addition to the early warning systems of the business.

Where a business already has this software Internal Audit can have an assurance role in confirming it is the right fit for he business and covers the most critical risks and vulnerabilities.

Internal Audits Role in Information Security Breach Detection

Internal Auditors are the eyes and ears of the Board and a pivotal aspect of the function is to constantly question.

Three key questions Internal Audit can ask about 'IT Security and Preparedness' to ensure data breach risks are managed. The questions are:

1. Is the organisation able to monitor network usage and application usage by all staff?
2. Is the organisation able to identify whether an attack is occurring at any point in time and whether it is affecting certain users or types of data?
3. Can the organisation isolate and restrict potential damage?

Internal audit can also play a key role in coordinating assurance efforts from all areas of the business. This may come from consultants, external auditors or Information Security Officer and/or a Data Protection Officer. An **end to end** opinion can identify critical weaknesses.

Conclusions
What does this all mean for Internal Audit

Proactively utilising cyber security data can help Internal Auditors **detect patterns** which in turn can highlight security issues that need to be addressed. Keeping on top of information security developments and regulations is one of a number of ways Internal Audit can demonstrate the added value provided to the business. Information security and data privacy risks cannot be evaded **BUT** they can be assessed and controlled:

- There is no ‘Magic Bullet’ or ‘Panacea’ which Internal Audit can provide to address all information and privacy threats. However, by leveraging some of the new technology, tools, analytics and AI, Internal Audit can help the business stay ahead of the threats.

A Forward Looking Internal Audit Team Knows That:

- **Data will continue to grow;**
- **Technological developments will continue to take place;**
- **Internal Audit needs to decide whether it is a follower or leader;**
- **Adding an edge / sector expertise;**
- **Data = knowledge and this equates to Insight;**
- **Data and information security spend – efficiency and economy;**
- **Considerations: privacy, cyber, resource; and**
- **Embrace the opportunity.**

Contact Information

MOORE STEPHENS

Anthony Blenkey

Director of Assurance & Advisory UAE and Qatar

E anthony.blenkey@moorestephens.com

T +44 (0)20 7334 9191 or +971 (0) 568742511

www.moorestephens.co.uk

Sources & References

Financial Times Lexicon

UK Information Commissioner's Office

TechTarget Essentials, A Guide for CIOs

The IAB Data Center of Excellence and the Data & Marketing Association (DMA)

Reuters

Juniper Research

Microsoft

The Institute of Risk Management (IRM)

Gartner

The Institute of Internal Audit (Global and UK))

Lloyd's of London

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Gemalto - Data Breach Level Index

ISACA

Computer Weekly 2016 and Wired

Institute of Internal Auditors (IIA) Standards and publications

The Institute of Internal Audit Global Technology Audit Guides (GTAGs)