Internal Audit Takes On Emerging Technologies
Introduction

The growing risks in technology

With data breaches in the headlines most days, executives are increasingly concerned about data privacy and security issues. The growing use of social media, mobile devices and cloud computing has introduced a higher threat of IT security breaches, misuse of customer data, and reputational damage.

Organisations are turning to internal audit and asking for help on managing the seemingly new and specific risks of emerging technologies.

In this paper, we examine the following threats and opportunities of emerging technologies:

- Smart devices/ technology
- Social media
- Cloud computing
- Cyber security

We explore the issues that businesses are currently facing, better practices we have observed that can be applied, and areas that internal audit can focus on to stay ahead of the trends.

In PwC’s 2012 State of the Internal Audit Profession Study, data privacy and security is one of the main risks identified by senior executives and heads of internal audit.

“Organisations are turning to internal audit and asking for help on managing the seemingly new and specific risks of emerging technologies.”
1. The cloud offers major benefits, but what about the risks?

Cloud computing has proved that its benefits extend beyond lower IT costs, less complex infrastructure, better flexibility and increased operating efficiencies. As the technology advances into the mainstream, organisations are finding that cloud computing can spur innovation by lowering the financial barriers to creating new products and services. However, without careful planning and consideration of market concerns, these gains can be overshadowed by a number of risks. Any organisation considering a move to the cloud must be aware of both its inherent shortcomings and its strengths in order to reap its full potential and value.

Heads of security are most concerned about data privacy in the cloud. In our 2012 Global State of Information Security survey, 32% of respondents say their greatest security risk is an uncertain ability to enforce the cloud provider security policies. Another concern cited by 11% of respondents is that data may be stored on servers shared with other companies. Because these servers can span different geographic locations (an approach known as multi-tenancy), sensitive information can be governed by multiple, and sometimes conflicting, jurisdictions.

Accordingly, significant security hurdles must be cleared before a business implements cloud computing. Organisations should carefully assess which of its applications and data are appropriate to move to a cloud environment. The company should rigorously evaluate the capabilities of any potential cloud services provider, including factors such as data security and privacy, compliance, availability, and scalability. At the same time, the portability of data and applications must be considered, to ensure that organisations can move to a new provider should an existing vendor fail to deliver agreed service levels.
2. Real-life examples of what can go wrong

Cloud computing technologies have been successfully implemented in many cases. However, there are several examples where it has resulted in disruptions to businesses operations, including:

- **Amazon Web Services** – technical issues resulted in outages of 36 hours for over 70 clients (against their marketing promise of 4.4 hours annually).

- **Sony PlayStation Network (PSN)** – network outage as a result of an ‘external intrusion’ led to the theft of personally identifiable information from each of the 77 million accounts.

- **Distribute IT** – a domain registrar and website hosting company where the environment was breached, destroying live data and all associated back-ups. This resulted in 4,800 websites being lost/unrecoverable, and in some instances, businesses closing.

3. Good practices for managing risk, particularly changing risk

Given the pace of change and maturity of this emerging and rapidly evolving technology, no single industry standard or best practice currently exists. However, a number of frameworks have been established based on existing outsourcing standards. These include Cloud Security Alliance’s **Cloud Controls Matrix** and ISACA’s **Control Objectives for Cloud Computing: Controls and Assurance in the Cloud**.

As cloud technology is increasingly adopted, new good practices in risk management and execution will certainly be required, as well as an industry-standard maturity model.

4. What should internal audit focus on?

To address the impact on the company’s risk profile, internal audit will need to rethink its focus on traditional IT and procurements, to include a potential shift in IT governance structures, challenges in the management of outsourcing risk, and the extent of compliance with federal and state privacy regulations. Internal audit can help the business assess, manage and govern the risks associated with cloud computing to ensure business benefits are realised. Key areas where internal audit may consider focusing are:

- **Contractual agreements**: Obtain a clear understanding of the responsibilities of the service provider, and determine what rights and recourse you have for the following: security breaches or incidents; defining and monitoring SLAs; specific contract requirements; and avenues for adherence to local and global regulations.

- **Access controls**: The cloud provider should prove it has implemented and enforced administrative controls to limit employee, partner/supply chain access to your information. It should also adequately investigate the background of employees who will have access to data, both logically and physically.

- **Certification and third-party audits**: Verify that service providers have some form of accepted third-party review of controls (SSAE16, ISAE 3402 or ISO 27001 certification). If possible,
seek independent reviews of their facilities and operations.

- **Compliance requirements:** Determine whether the supplier meets your compliance needs. A critical factor will be the geographic locations of the provider’s servers; be aware of laws that affect your data in any country in which it may reside or where data is being processed.

- **Availability, reliability, and resilience:** Enact agreements and responsibilities for measurable service levels in availability and reliability.

- **Back-up and recovery:** Ensure that disaster recovery requirements are clearly defined and responsibilities are well understood. Understand a provider’s capabilities in this regard before you engage them.

- **Decommissioning:** Data will be securely deleted once it is no longer needed.

- **Portability:** Determine whether you can easily move data and applications to another cloud provider or migrate data and applications back to an on-premises environment, if necessary. Before selecting a cloud provider, make sure that it does not use specialised or proprietary technologies

> Cloud computing has proved that its benefits extend beyond lower IT costs, less complex infrastructure, better flexibility and increased operating efficiencies
1. **Mobile devices are becoming smarter, and presenting greater risks**

Most organisations aim to be flexible and meet business requirements by providing mobile devices to their teams. At the same time, they need to balance the value against the risk of smart devices. The main risks companies need to be considering are the following:

- **Increased risk of information loss** – a security incident is easier with a smart device because of the theft or loss of that device.

- **Monitoring** – an ever-increasing range of malware and espionage software is being created for mobile devices.

- **Awareness and communication** – it’s increasingly important to educate staff and other users about the use of poor security practices (e.g. weak PINS and passwords, insecure configuration settings) by those who use their own devices at work.

- **Treatment of devices as any other end-point** – routes into the corporate network are created by mobile device architecture, which could result in the leakage of highly sensitive information.

- **Education of IT staff** – IT team members may not be experts in mobile device management and may not configure them securely, patch frequently, etc.

2. **Real-life example of what can go wrong**

In a high profile case in 2010, an Apple employee lost an iPhone prototype, which resulted in a security breach of approximately 114,000 security records including those of CEOs, military officials and politicians. The information disclosed included subscribers’ email addresses, as well as IDs used to authenticate subscribers to the network. While to date we have seen fewer thefts of mobile devices than of laptops, research confirms that employees are 15-20 times more
likely to lose a mobile device than a laptop (due to their size). This, coupled with the fact that mobile malware increased by 250% in 2010, means that we expect to see a large increase in mobile data breaches.

3. Good practices for managing risk, particularly changing risk.

Organisations’ risk appetites vary greatly, but one effective way of helping manage the risk related to smart devices is to select a Mobile Device Management Solution that is appropriate for your organisation. Our clients implementing this practice tend to choose a vendor based on trusted research publications.

Organisations should work closely with the selected vendor to design a secure architecture for their environment as well as secure policies, device protection and device management. The Defence Signals Directorate has produced guides for smart devices that are very helpful in this regard. Finally, organisations should look to develop complete and thorough mobile strategies, mobile policies and procedures and mobile

4. What should internal audit focus on?

Internal audit needs to consider the following areas with regard to smart devices:

- **Smart device strategy** – review and confirm that mobile device solutions are in line with the corporate strategy and will help the business to meet its needs by gaining maximum benefit from mobile devices.

- **Policy, procedure and awareness** – investigate the policies, procedures and awareness programs in place, their currency and relevance, and staff’s familiarity with their responsibilities to protect corporate information.

- **Technology review** – review the technology used for mobile device management as well as the devices themselves to ensure they are secured in line with industry leading practice and the organisation’s security policies. As ever, a security review is only ever meaningful at a single point in time, and internal audit will need to keep a close eye on mobile security developments, including the introduction of new malware.

Most organisations aim to be flexible and meet business requirements by providing mobile devices to their teams.

"Most organisations aim to be flexible and meet business requirements by providing mobile devices to their teams"
1. Social media is being extensively adapted for companies’ use, internally and externally

There is significant potential for organisations to use social media to connect with both their customers and their employees, and this opportunity should not be underestimated. By connecting with customers/clients through this new channel, organisations are able to build brand loyalty and easily share ideas. However, with this opportunity comes an increased risk, as follows:

- **Negative brand image:** Social networking gives customers an outlet to share comments about a company and its products and services. This can be valuable feedback if constructive; but if taken too far or done maliciously, it can negatively affect a company’s brand image.

- **Data loss:** With employees having a direct connection to so many people, there is an increased risk that proprietary information could be accidentally or intentionally leaked to the general public. These multiple connections can also lead to customer data loss due to hacking or malware.

- **Distribution of malware:** With the increased connectivity from social networking, even a minor system hack can spread quickly. Services such as TinyURL, Bit.ly and Cligs have become very popular as they allow URLs to be displayed in a more succinct form by Twitter users. But while useful, these can bring malware with them.

2. Real-life example of what can go wrong

Recently, Cligs was the subject of a hacking incident where more than two million URLs were changed to a single URL directing users to an article about Twitter hash tags. Graham Cluley, a senior technology consultant at Sophos, warned that the incident could have been much worse. “It is not yet apparent what the hackers’ intentions were, but they could just as easily have redirected millions of shortened URLs to a website hosting malware.”

3. Good practices for managing risk, particularly changing risk

- **Awareness programs** – educate staff on what is acceptable (via a code...
of conduct) and define who is responsible for particular types of communication.

- **Policy & Procedures** – establish policies for security, social media and ethics, and include reference to them in employment terms and conditions.

- **Communication** – pilot any new technology internally first, then let people know what is acceptable or not. Ensure regular communication between employees and the social media team to promote awareness about what is happening in the social landscape and within the company.

- **Security technology** – evaluate and use technologies to control, monitor, and enforce your policies – especially in regulated advice-based businesses.

- **Risk assessment** – monitor the use of social media and continue to challenge the risks, risk management and the contingency plans in the event of a negative event.

- **Time quotas** – enforce time limitations for the use of social media to align with your risk appetite and profile.

- **Crisis management and mitigation** – implement formal plans, including scenarios.

4. **What should internal audit focus on?**

Internal audit should be asking these questions:

- Is the social media strategy clear? Does the organisation understand how its people and customers are using social media in relation to the organisation?

- How are we using social networking technologies, both internally and externally? Are we gathering data from these technologies to help drive business strategy and to monitor our brand in this part of the market?

- Have we defined metrics based on social networking analysis concepts such as the following?
  - How does the use of social networking affect your brand?
  - How does it increase the risk of corporate, employee and customer data loss?
  - How does it increase the risk of e-commerce transactions?

> There is significant potential for organisations to use social media to connect with both their customers and their employees
1. **Cyber security has introduced many previously unknown risks**

The traditional IT security controls used in many organisations aim to create strong borders to stop attackers. They do not account for a multitude of internet channels, complex relationships with partners and providers, social media and the explosion in mobile access.

Organisations need to have a clear understanding of the value of their information, where that information resides, the financial impact of loss or theft, and the likelihood that an attacker will be interested in their data. With the move online, information may be inside the organisation’s systems, on employees’ mobile devices, managed by IT service providers, communicated to business partners, or even downloaded to customers’ own devices as they make use of online services.

2. **Real-life examples of what can go wrong**

The media continues to report a number of high-profile attacks on both large and small organisations, to access and remove sensitive intellectual property, financial information and private customer data.

One of the world’s leading IT security companies publically admitted it had lost the computer code at the heart of its security software. This gave rise to widespread concern as its software is used to control access to organisations’ most important and sensitive information. So the organisation’s most valuable information was able to be stolen by a remote attacker through a series of undetected (at the time) targeted attack.

A common theme is that these organisations rarely understand the real risk to their information until after the event, leaving them to deal with high-impact and often reputation damaging business incidents not previously on the corporate risk radar.

3. **Good practices for managing risk, particularly changing risk**

The first step towards countering the threat is to determine where valuable
The first step towards countering the threat is to determine where valuable business information resides. Once the organisation is aware of what information is valuable and where it is stored, it can carry out a risk analysis and introduce effective security controls.

The aim is to guard against both well recognised threats and less likely events with a high potential impact, including the disclosure of sensitive commercial information — from product innovations to acquisition targets.

Then, with a risk management framework in place, it’s essential to continually review the threat environment, adjusting your controls to meet what are fast-evolving risks. Every time another organisation has a serious incident, lessons should be applied to your own organisation to decrease the likelihood that you will be next.

4. What should internal audit focus on?

Internal audit should be asking these questions, at a minimum:

- Have repositories of important information, including potential business differentiators, been identified?
- Is there a central register of important information assets?
- Has the risk to these information assets been calculated and an appropriate risk appetite agreed?
- Have information assets in the IT networks and systems been mapped?
- What internal security controls exist to segregate important information and ensure only those who need to access it can do so?
- Are customers’ expectations of privacy and security increasing and responses adapted accordingly?
- Is the organisation constantly reviewing the threat environment and controls, and adjusting counter-measures accordingly?
- Does the organisation have an action plan to respond to a loss of sensitive or damaging information? Is it linked to crisis and media management plans?
What should Internal Audit do next?

Assessment and awareness

- Help the organisation to develop a strategy that defines the ‘as is’ and ‘to be’ processes for assessing service level agreements, monitor its implementation and document and evaluate metrics to measure progress towards objectives. Consider the frequency of review of the strategy to deal with changing and emerging risks.

- Develop an education plan to continually update internal audit staff on emerging technologies.

- Engage an expert adviser to keep you abreast of the rapidly evolving trends and practices in technology, enterprise risk, governance, security, and privacy relevant to the respective technologies.

- For existing implementations (e.g. for cloud), engage an independent party to help assess your provider’s controls, or ensure that your provider engages a independent party to provide this assurance.

Information assets

- Create and maintain a central register of important information assets.

- Calculate the risk to these information assets and agree an appropriate risk appetite, which has been approved by management and the board.

- Map your information assets to the organisation’s IT networks and systems.
**Security and access**

- Review your internal security controls to ensure important information is segregated and only accessible by authorised individuals.

**Response to threats**

- Implement a process whereby your organisation constantly reviews the threat environment and adjusts controls and counter-measures as applicable.

- Review your action plan to respond to a loss of sensitive or damaging information and determine whether it is linked to crisis and media management plans.

**Social media policies**

- Implement/review existing policies and procedures relating to social media, data security etc.

- Communicate the data classification to your employees to ensure they know precisely what is and is not sensitive information. Confirm with your marketing or communications team whether they have taken responsibility for your company’s public social media footprint; or whether the organisation needs a social media strategist and a communications manager.

- Revisit your separation agreements to ensure they cover protection and maintenance of ownership of intellectual property and social identities.
George Sammut                  george.sammut@mt.pwc.com
Partner                      (+356) 2564 7608

George joined PwC in 1987, and is now the Partner leading the Systems and Process Assurance service line that, amongst other services, leads the delivery of internal audit solutions to clients. George was a pioneer in information systems auditing and security in Malta, having worked in this area for the last 15 years. He has lectured frequently on many areas of data protection, internal controls and information security, including Security Management, Access Control Architecture, Security Value Management, Disaster Recovery and Business Continuity.

George has a BSc (Hons) degree in Data Processing, is a qualified accountant, a Chartered Engineer, a member of the British Computer Society, a member of the Institute of Financial Accountants, Certified in the Governance of Enterprise of IT (CGEIT), and Certified in Risk and Information Systems Control (CRISC).

Gordon Micallef              gordon.micallef@mt.pwc.com
Senior Manager               (+356) 2564 7014

Gordon has over 12 years of information technology and information security assurance and advisory experience. He has led several IT internal audits and reviews, including assessing controls over operations and management, application change control, computer operations, security administration, physical and logical security, and disaster recovery planning. He also led several IT governance improvement assignments across large organisations in Malta.

Gordon is a Certified Public Accountant (CPA), Certified Information Systems Auditor (CISA), Certified in the Governance of Enterprise of IT (CGEIT), and Certified in Risk and Information Systems Control (CRISC). He is the founding member and Past President of the ISACA Malta Chapter.

Nathan Gatt                  nathan.gatt@mt.pwc.com
Manager                      (+356) 2564 7035

Nathan has information systems security and audit experience and currently provides IT audit support to clients in various industries. Nathan has been involved in reviews of system-based and manual controls in a number of industries (e.g. financial, remote gaming, pharmaceutical industry). He is currently responsible to carry out web application security assessments and infrastructure penetration testing.

Nathan is a Certified Information Systems Security Professional (CISSP) and a Certified Information Systems Auditor (CISA). He is also active in a number of special interest groups related to various information security domains.
This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2012 PricewaterhouseCoopers. All right reserved. PwC refers to the Malta member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.