LexisNexis Risk & Compliance paper

Emerging technology and its impact on Governance, Risk and Compliance (GRC)

Aaron Cleavely-Millwood,
Risk & Compliance Product Specialist,
LexisNexis Pacific

Released February 2013

LexisNexis®

The speed and complexity of this changing, technologically-driven business environment has pushed governance processes, control and risk management to the fore as a key concern.

Emerging technology and its impact on GRC

Technology is changing the way businesses and individuals are interacting, communicating and sharing information.

- Nearly 1 billion people used Facebook in June 2012
- Twitter generates over 200 million tweets per day
- 100 billion searches are generated each month via Google
- The volume of business data worldwide doubles every 1.2 years

The speed and complexity of this changing, technologically-driven business environment has pushed governance processes, control and risk management to the fore as a key concern.

A 2012 KPMG governance report identified two key areas of risks posed by emerging technologies. The first risk identified was information data privacy and security, followed by leveraging social media and data to shape real-time business decisions. The report also found that the top concerns of audit professionals included risks around governance, processes and control, IT risk and legal/regulatory compliance. Only six percent of the survey's respondents felt satisfied that their company's governance process and controls were keeping pace with technological change.

This fast changing environment is calling for GRC to permeate the whole organisation through proactive risk management, with KYC/KYS emerging as an important tool to be utilised beyond its traditional application.

58% of audit professionals identified risk around **information data privacy & security** as causing them the most angst

28% identified **social media** (impact on reputation & customer strategy)

6% felt satisfied that their company's **governance process and controls are keeping pace with technological change**

Emerging Technology Spotlight

Bring your own Device (BYOD)

The BYOD revolution represents a mobile and flexible working environment which offers significant productivity enhancements for 'on-site' GRC tasks.

- 80% of employees used own devices at work
- 53% of companies condone BYOD
- 63% of employees believe BYOD positively influences their view of the company

Threats & Risks

- Data loss and leakage
- Data held on personal devices might be discoverable and unsecure
- Responsibility of injury from the use of a BYOD device, e.g. repetitive stress injury
- Unsafe disposal of devices
- Impact on an individual's content if the device is wiped by the action of a company employee

Reducing the Risk

- Remote locking and deleting of devices, e.g. wiping iPhones remotely
- Mobile Device Management (MDM)
- Education

Big Data

Big data is a collection of data sets so large and complex that they become difficult to process using on-hand database management tools or traditional data processing applications. Big data is a key driver of innovation, productivity, competition and transparency.

> "It's important to recognise that this is an information revolution more than a technology revolution"
>
> *KPMG Audit Committee Institute Report, 2012*

Threats & Risks

- Tools which enable more sophisticated data mining and pattern analysis mean that it is possible to identify 'interesting' information that was previously unattainable
- Cost concerns and ROI accountability due to the cost of managing a large database
- Privacy breaches
- Copyright infringement

Reducing the Risk

- Governance
- Obtain consent
- Anonymise
- Identify and avoid or secure 'toxic data' such as credit card numbers
- Third party content (copyright)
- Data handling policies and policing
- Effective due diligence process

Surveillance & Monitoring

Ubiquitous technology connected to the web is the ultimate panopticon. Almost everyone carries a device which constantly sends information about that person's location, activities and interactions.

The adoption of employee monitoring tools is growing:

- keystroke monitoring
- email logs
- web activity

Threats & Risks

- With millions of transactions occurring each day there is a need for sophisticated transaction monitoring systems to identify unusual and/or suspicious behaviour
- Emails and internal trading must be monitored to ensure compliance with trading blackouts
- The legal complexities of surveillance – some surveillance is most likely restricted by law and in some instances it may be required by law
- Significant risk of breaching employee privacy
- Negative impact on employee morale

Reducing the Risk

- Deploy state of the art transaction monitoring systems and with rules configured by subject matter experts
- Continually review and fine tune transaction monitoring systems
- Ensure compliance with policies and procedures
- Ongoing oversight and independent reviews
- Use social media monitoring tools to detect insurance fraud
- Effective due diligence – KYC/KYE

Intellectual Property & Information Privacy

Intellectual Property (IP) Protection and Information Privacy are closely linked. IP is an important asset in today's knowledge economy and should be strategically managed.

Threats & Risks

- Not differentiating between personal information that is required by law to be collected and information that is not
- A 'collection notice' is not provided (as is required by Australian law)
- Sensitive information is collected but is not recognised as being sensitive
- Risk of legal noncompliance if information is used for another purpose or disclosed without authority
- Risk of privacy complaints if there is legal noncompliance or the public is surprised by a use for another purpose or a disclosure
- The most commonly stolen IP is customer databases

Reducing the Risk

- Block USB ports to reduce data loss
- Monitor emails that employees send to ensure data remains secure
- Force change of password regularly
- Educate staff on not sharing passwords
- User access reviews to ensure password
- Ensure that data protection and data destruction policies are followed
- Effective due diligence: KYC/KYE/KYS/KYSS

Cyber Security

Information security as applied to computers and networks is referred to as Cyber Security. The *2012 Cyber Crime and Security Survey Report*, commissioned by CERT Australia, revealed that cyber-attacks are now more coordinated and targeted for financial gain.

The cost of cybercrime is $5bn per year and growing:

- SMEs reported individual loss of $650m due to cybercrime
- 44% of attacks originating from within organisations

Threats & Risks

- The most common form of cybercrime is theft or vandalism by current and former employees
- Cloud based storage raises additional risks as data is held by a third party and potentially stored in a foreign jurisdiction (the US Patriot Act has raised concerns in the Pacific Region)
- The denial of service attacks can be problematic for businesses with a heavy online presence or critical business functions using a web interface
- Breach of confidentiality information
- With millions of transactions occurring each day there is a need for sophisticated transaction monitoring systems to identify unusual or suspicious behaviour
- Put internal monitoring systems in place which track emails and internal trading to ensure compliance with trading blackouts

Reducing the Risk

- Ensure firewalls are in place to protect your data
- Use email blockers to filter spam emails
- Ensure employees are unable to download software files from unknown sources
- Prevent employees from accessing certain 'unsafe' or 'restricted' websites
- Inform customers of the importance of protecting their identities
- Deploy state of the art transaction monitoring systems
- Effective due diligence – KYC/KYE/KYS
- Regular reviews of TMP effectiveness
- Ensure compliance with policies and procedures
- Ongoing oversight and independent reviews
- Use social media monitoring tools to detect insurance fraud

New Payment Technology

New technology is emerging with contactless payment systems such as credit cards and debit cards, key fobs, smartcards or other devices that use radio-frequency identification (RFID) for making secure payments . According to RBA statistics, there are an estimated $470 million in cash transactions under $35 million moving through the Australian economy each day, or around $170 billion per year. This form of technology is to be adopted by most businesses in 18-24 months.

Forms:

- Contactless cards – go money and pay wave
- Peer to peer payment via mobile phone
- Kaching

Threats & Risks

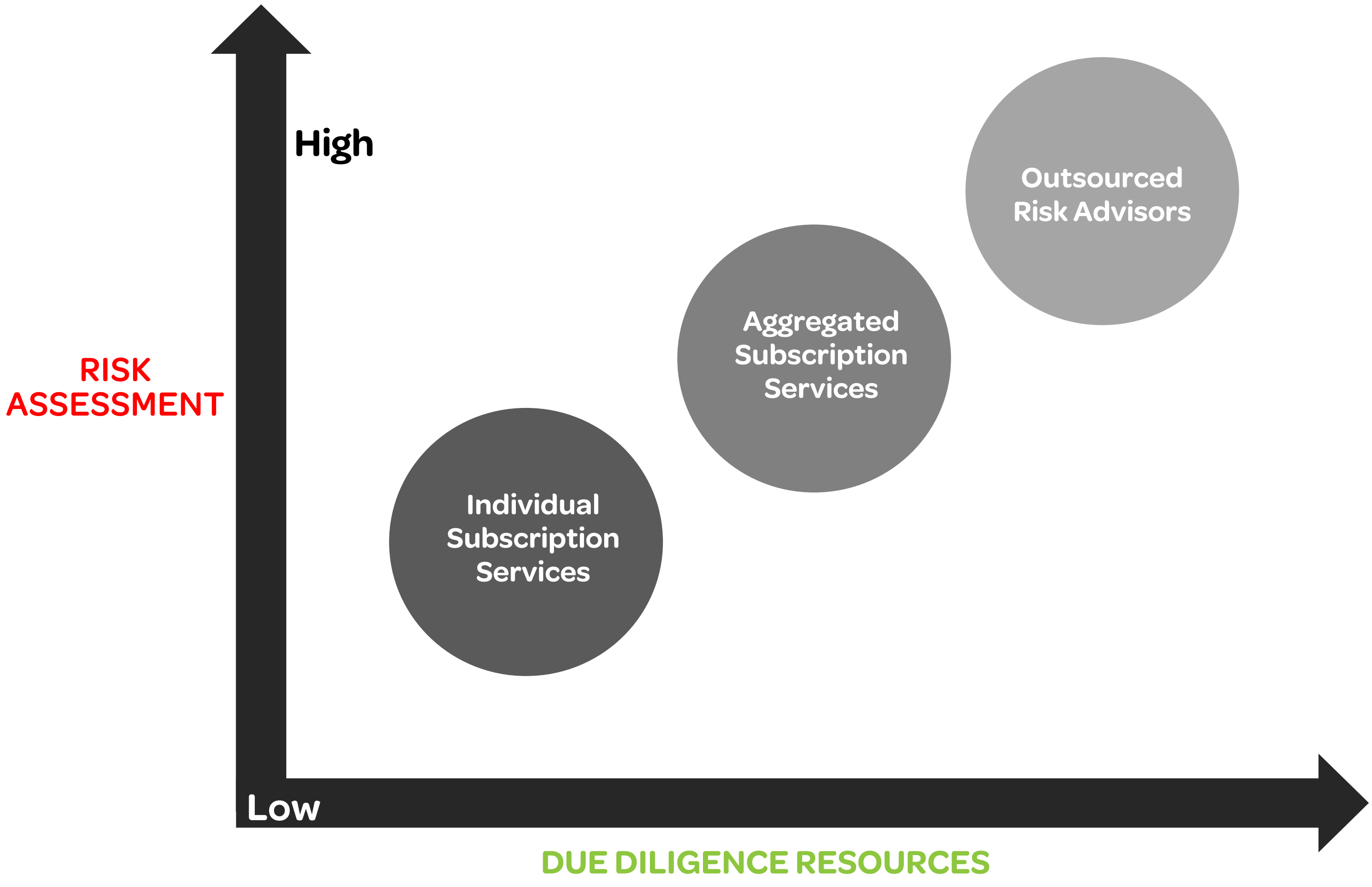
- The RFID chip feature comes switched on and can't be switched off, the consumer has no choice as the card comes with the functionality
- No authentication is performed to confirm the authority of the person who is using the card (i.e. no signature, no PIN)
- Transactions may or may not involve visual notification to the cardholder, who may or may not notice any such display
- Data privacy concerns

Reducing the Risk

- Know your limits
- Be app savvy
- Put security measures in place
- Wipe your old phone

The Future of GRC

Emerging GRC Solutions & Tools



Emerging Risk & Role of Enhanced Due Diligence

Effective Due Diligence is evolving into a major risk mitigation and prevention tool that goes beyond legislative and KYC/KYS requirements, to other governance risk and compliance elements including corporate security, legal, strategy, credit, risk, fraud and procurement.

For more information:
Visit www.lexisnexis.com.au/riskandcompliance or call 1800 772 772

LexisNexis Pacific

LexisNexis® Pacific is the leading provider of local and international news, business, tax and legal information, using leading-edge technology, tools and digital solutions. Both in Australia (www.lexisnexis.com.au) and New Zealand (www.lexisnexis.co.nz), LexisNexis Pacific works in close collaboration with its customers to provide content enabled-workflow systems for professionals in law firms, corporations, government, law enforcement, tax, accounting, academic institutions and compliance assessment.