KPMG

Derbyshire Audit Forum

Venue – Derbyshire County Council

26 January, 2017

John Cornett

Tony Crawley

Agenda

14:00

Welcome and Introductions

14:00 – 14:30

What makes an effective Audit Committee?

14.30 – 15.00

Risk management – the basics

15.00 - 15.20

Break

15.20 – 16.00

Cyber security

16.00 - 16.40

Hot Topics

16.40 - 17.00

Closing remarks
Future events?

17:00

Close

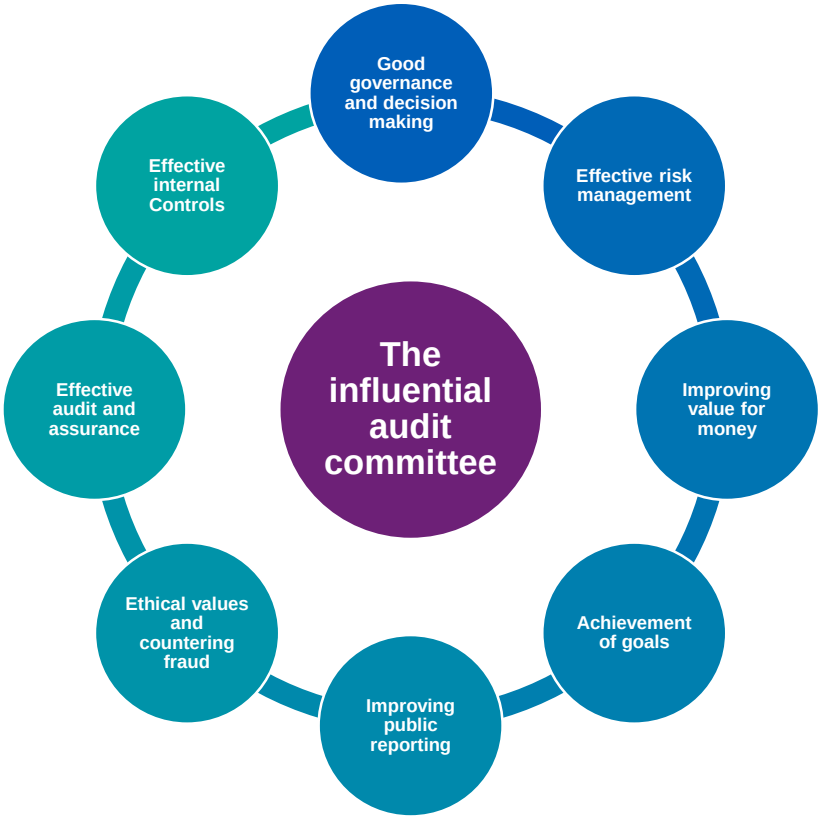
KPMG

Effective audit committees

Effective Audit Committees

‘Audit Committees are a key component of corporate governance. They are a key source of assurance about the organisation’s arrangements for managing risk, maintaining an effective control environment, and reporting on financial and non-financial performance.’

CIPFA



Audit Committees: Practice Guidance for Local Authorities and Police. *CIPFA December 2013*

Effective Audit Committees

What do you think makes an Audit Committee effective?

Effective Audit Committees

Characteristics of an effective Audit Committee

- **Membership –** Ensuring that the audit committee has the expertise and experience to provide robust oversight of financial reporting, audit quality, and other risks on the committee's agenda.

- **Active involvement –** In-depth knowledge of the organisation gained from (pro)active engagement and genuine interest in the organisation (beyond the boardroom).

- **Driving the audit committee's agenda –** The audit committee must shape its own agenda to ensure that it's risk-based, focused, and manageable.

- **Effective communication –** Open lines of communication with senior and middle management, internal and external auditors, and the full board based on mutual trust and constructive debate. "White space" time on the agenda for open dialogue.

Effective Audit Committees

Characteristics of an effective Audit Committee

- **Getting the right information –** Information provided to the audit committee must be relevant, concise, and timely.
- **Informal meetings –** Informal and ad-hoc meetings (in between regularly scheduled meetings) are essential to stay fully informed.
- **Tone at the top –** Sensitivity to the tone at the top of the organisation – and, indeed, throughout the organisation.
- **Leadership –** The attitude, skillset, and engagement of the audit committee chair are essential to achieving all of the above – which collectively drive the audit committee effectiveness.

Effective Audit Committees

Agenda management

- **Is there a plan for the year to enable the Committee to meet its ToR?**
- **Who sets the agendas?**
- **Do reports map to the terms of reference?**
- **Do all Committee reports pass the ‘so what’ test?**
- **Do you assess whether you get the necessary assurance from each item?**
- **Is it clear who attends the Committee meetings and what you want from them?**
- **Do attendees know why they are there and the assurance you are looking for?**

Effective Audit Committees

Meetings

- **Is there sufficient debate?**
- **Are decisions open?**
- **Do Committee members contribute evenly?**
- **Is the focus on quality of discussion rather than quantity of topics covered?**
- **Is there enough challenge and fresh thinking?**
- **Does the Committee take time to self-reflect, and ask for independent views?**
- **Do you recognise any of the issues in the ACI paper?**

Effective Audit Committees

The Committee's accountability for its role

- **How do you provide assurance that you have delivered your ToR?**
- **Have Members' training needs been assessed and addressed?**
- **What impact has the Committee had?**
- **Have you assessed your effectiveness, and taken action where needed?**
- **Do you provide assurance that you have met your ToR – eg an Annual Report?**

KPMG

Risk management (and the AGS)

Risk management - the basics

Simply……

The means to better identify and manage risks in a more co-ordinated manner in order to meet goals and objectives

Risk management is NOT…

…One event

…One size fits all

…Just about being compliant

…About eliminating risk

…The only answer to improving performance

Risk management IS:

…A series of actions

…About understanding your corporate objectives and how risks could affect their achievement

…A journey to improving performance and operational excellence

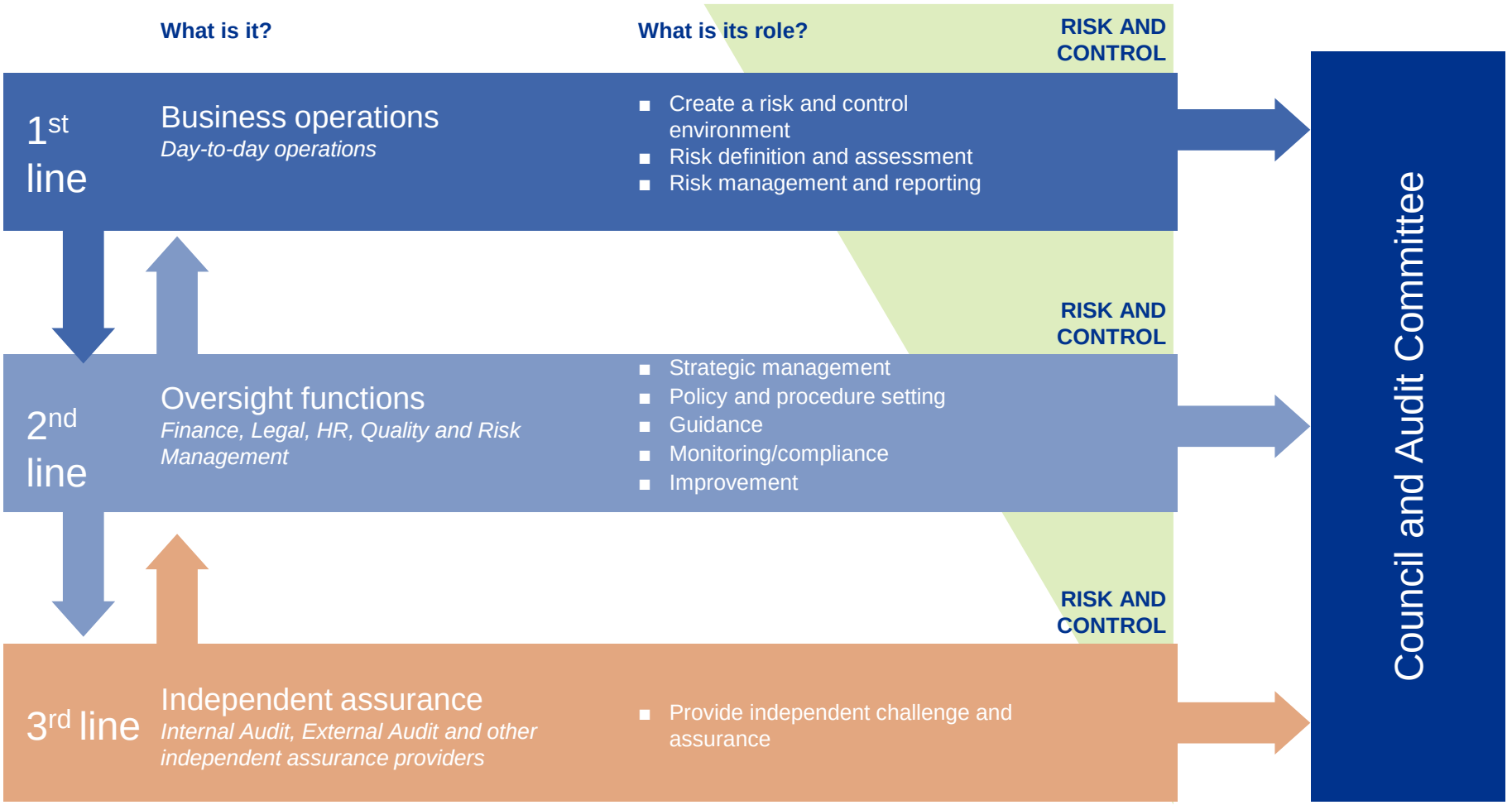
…Subject to the integrity of those accountable

…More than a process: “enterprise-wide” - culture, structure, policies, practice

…Owned by the Board – Practised by management

Risk management – the basics

An assurance structure includes each of the following three lines of defence:



Risk management - common issues

CONTENT	1	The risks contained in the risk register often don't reflect the real risks the organisation is running – identification/ measurement is wrong
	2	The risk assessment process by itself won't help manage risk better – you've got to understand the control environment and behavioural aspects
	3	Reporting of risk information is still largely compliance driven with observations focusing on the priority of risks rather than on control and improvement actions or developments of the risk management process itself
PROCESS	4	Selling the business case for risk management is still in the 'too hard' tray – many organisations don't have dialogue with their key stakeholders on risk management - investment and return are not clear, risk appetite is not known
	5	In many organisations executive management need to take more sponsorship and accountability for risk information and actively use it to improve performance and compliance
	6	Often there is no clear framework that co-ordinates risk management and internal control across the organisation – this can lead to confused management structures and policies surrounding risk and lack of focus for internal audit and assurance on what matters

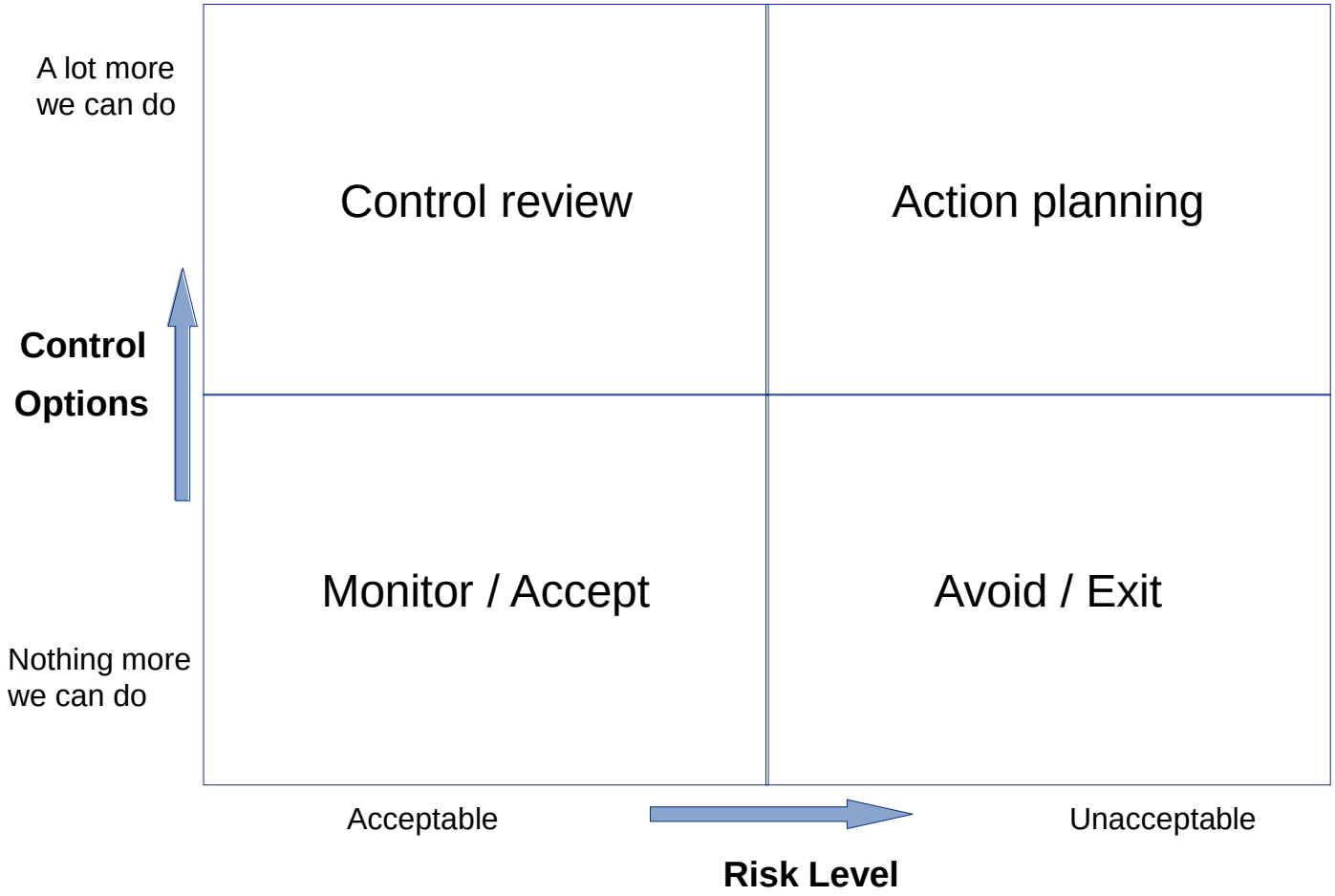
Do you recognise any of these?

Risk management - choices

Risk appetite and control options

Your risk appetite is a key driver of your response to risks. But:

- **It depends on the level of risk**
- **It depends on your control options – which is partly driven by internal vs external considerations**



Risk management and the audit committee

The view from CIPFA

The role of the audit committee is to:

1) Seek assurance over governance risk
2) Keep up to date with the risk profile and the effectiveness of risk management;
3) Monitor the effectiveness of risk management arrangements and embedding good practice

Assurance over risk management is key to **THE** key element underpinning the Annual Governance Statement.

The audit committee should not manage or score the risks

Annual Governance Statement

What is it?

- **A review of the effectiveness of the council's system of internal control across all its activities.**
- **A Public report – promotes accountability.**
- **An open and honest self-assessment.**
- **An action plan to address significant and potentially significant risks.**

Annual Governance Statement

A good AGS should be ....

- **Open and honest**
- **A clear statement of actions**
- **Built upon a robust assurance framework**
- **Approved and owned at corporate level**
- **Reviewed and approved by Members separately from accounts**

Annual Governance Statement

What do you need to review the Annual Governance Statement (AGS)?

- **Knowledge of the governance framework of the organisation**
- **Understand the assurance framework that underlies the AGS**
- **Knowledge of the risks and internal control issues that have emerged during the year**
- **Be satisfied that the review of effectiveness is adequate**
- **Be satisfied that the action plans are realistic and meaningful**

KPMG

Cyber risk

Cyber risk - the key questions

High Level Question	Supplementary Questions
How secure are you currently?	What have been the most serious security and privacy incidents that you (and your peers) have faced in the past 12 months, what have you learned from those experiences, and what are you now doing differently to prevent them from re-occurring?
Are you getting more or less secure?	What key indicators are on your security dashboard, how is the organisation achieving those objectives, and how does this compare to your peers?
How do you set priorities and risk appetite ?	What is your organisational risk appetite for downtime, data loss and privacy incidents, how do you set your appetite level, and how are you tracking against that? What are the 'crown jewels' that require the highest levels of protection? Which business processes are critical to survival of the organisation?
How are you organised to manage the issue?	How is your first line and second line of defence set up? How do you report on the risk? How do you co-ordinate across multiple responsible functions?
Are you spending at the right level? And getting value for money for that spend?	What are you spending on security over the next three years? Is it enough to appropriately respond to the threat? Where are you under-invested and where can you make savings? Can you defend your investment compared to your peers?
How do you manage third party suppliers?	How do you ensure your suppliers (and their suppliers in turn) do not expose you to unacceptable cyber risk?


Cyber-Extortionists
Targeting the Financial
Sector Are Demand
Ransoms
Millions affected after cyber attack on HSBC
HSBC's websites across the world have been hit by one of the la
Caught, cyber bank
robbers who tried
siphon off milli
JPMorganChase
STATEMENT
"Companies of our size
unfortunately experience
cyber attacks nearly
every day.
LAW360
News, cases, companies, firms
'Cryptolocker' Virus Holdi
Data For Ransom
By Y. Peter Kang
ROBBED
BY CYBER
HACKER
Conmen who stole TalkTalk custo
details are raiding their bank accounts
By Katherine Rushton
ASHLEY
MADISON®
Life is short. Have an affair.®
Get started by telling us your relationship status:
Please Select
See Your Matches »
Morgan Stanley Acknowledges Insider Breach
A former financial adviser allegedly stole 10 percent of the company's 3.5 million Wealth Management customers' account information.
By Jeff Goldman | Posted January 07, 2015
Share
Morgan Stanley this week began notifying almost 10 percent of its
clients that an employee had stolen their

Ransomware attack

Background

Email Received

- A member of Lincolnshire County Council opened a malicious email disguised as an invoice on the 26th Jan 2016.
- The email was opened and the malicious software was downloaded.
- The type of attack is known as a “zero day” attack. This is when the malware enters the system it can propagate itself easily as the antiviral software is unfamiliar with the software.

Data Encrypted

- Once on the system, all files on the council’s server were encrypted becoming inaccessible to those wishing to use them.
- The types of data seized includes: names, addresses, and medical conditions documented and dates of birth.
- The Council reported that there was no evidence that any of this information has been stolen.

Ransom Received

- The council received a ransom demand of £350 equivalent of the online currency, Bitcoin. The council refused to pay up.
- This was initially reported to be a much lager sum of £1 million.
- Once paid, the encrypted data would, in theory, be released.

Computer shutdown

The council was forced to suspend all use of their servers causing many services to be reverted back to pen and paper methods. Two days later, services were resumed as normal. No data appears to have been lost or stolen during the attack.

BBC Sign in News Sport Weather iPlayer TV Radi

NEWS

Home UK World Business Politics Tech Science Health Education Entertain

England Regions Lincolnshire

Lincolnshire County Council hit by £1m malware demand

29 January 2016 | Lincolnshire

HOME NEWS JOBS EVENTS PROPERTY SHOP BUSINESS COLUMNS VIDEOS Search

Home » Government

Police investigate Lincolnshire County Council 'ransomware' attack

Cyber Essentials – Would it have saved Lincolnshire County Council?

1 February 2016 | Written by Rallpm Security

Leave a Comment

Cyber Essentials is a UK Government driven scheme which is designed to help businesses of all size reduce the risk and impact from malware attacks. It is mandatory for those who provide services to the MOD. Cyber Essentials is becoming mandatory for those who provide services to any other government department – including local government and councils.

This is a good thing.

Despite there being some criticisms of Cyber Essentials, the scheme does what it says on the tin. It helps businesses prevent things like ransomware knocking them out.

Sadly, not every government department practices what they preach.

Lincolnshire County Council – Hit by ransomware Jan 2016

Around 26 January 2016, Lincolnshire County Council was hit with a ransomware attack. Initial reports from the BBC claimed the demands were for £1m. However by the end of the week this had been corrected to the more *normal* £300.

Ransomware can be devastating for home users. It has the potential to destroy priceless data. Few home users take proper back ups and end up having to pay. This means there is a lot of money to be made.

Organisations are different. The assumption is they will have backups. There is also an assumption they will never pay. This all means criminals very rarely target businesses with ransomware. What is likely to have happened is simply a user made a mistake with their email.

This happens a lot. It is also one of the reasons why Cyber Essentials was created and why it is so valuable for businesses.

Would Cyber Essentials Have Helped?

Within the Cyber Essentials framework there are five security control areas. These are the foundations of good security.

TechTank Late

Ransomware shuts down UK council

The Register

Biting the hand that feeds

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS

Security

Pay up, Lincolnshire, or your data gets it. Systems still down after ransomware hits

Council has shut down entire IT network to prevent spread

Cyber extortion is a growing threat

Warwick Ashford
Security Editor
01 Feb 2016 10:25

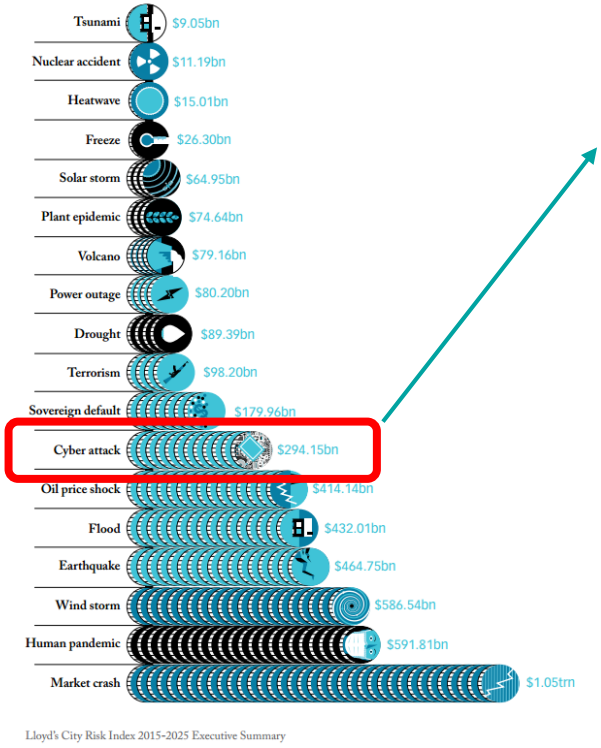
Security industry warns of increas attacks as Lincolnshire County Co ransomware demand

What was the impact?

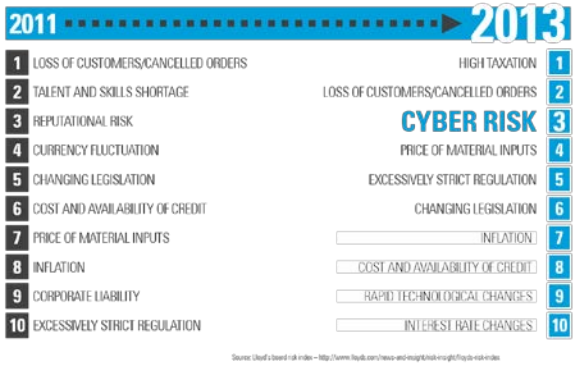
- The council suffered reputational damage;
- Library systems down (books were manually stamped);
- Online booking systems failed;
- Council main site halted;
- Financial losses;
- Productivity stifled.

What did they do about it?

- Lincolnshire County Council acted as soon as the malware was detected preventing further damage
    - Therefore, only a small amount of their data was affected.
    - The Council had everything backed up so data affected could be restored.
- They worked with an outsourced security company to get their services back and running.
- The Council said it had notified the Information Commissioner's Office (ICO) about the incident, but said no personal data had been compromised.



Lloyd's City Risk Index 2015-2025 Executive Summary



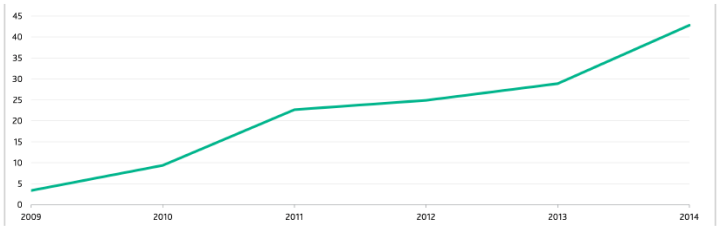
CHANGES

RISK RANKING

Exhibit 2

Detected Cyber Incidents Are Rising at a Fast Pace

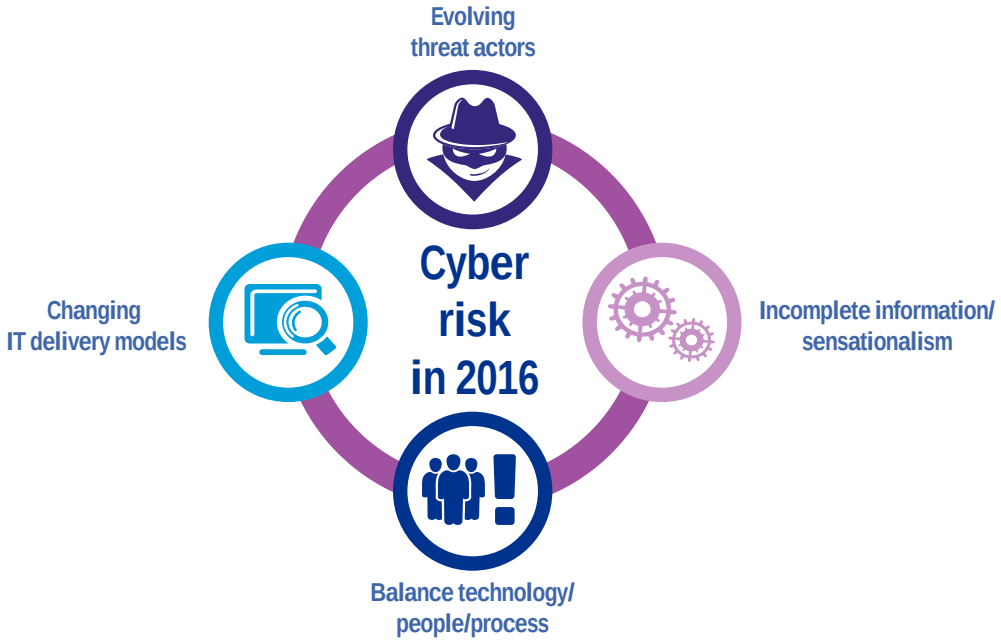
Millions of incidents



Source: PWC. Managing Cyber Risk in an Interconnected World, 30 September 2014; page 7.

Cyber Security Landscape

This is a “wicked” problem – multi-dimensional, unpredictable, intangible and constantly changing



Cyber Threats - It's a connected world

Who is being targeted?

WHO WOULD WANT TO TARGET US AND WHY?

THE INSIDER
Intentional or unintentional
Motivation: grudge, financial gain
Business impact: reputational damage, financial loss, regulatory censure

COMPETITORS
Competition or rivalry
Motivation: competitive advantage
Business Impact: competitive disadvantage

ISSUE MOTIVATED HACKERS OR 'HACKTIVISTS'
Attention or popular causes, may be / work with investigative journalists
Motivation: dynamic and unpredictable, potentially issue motivated
Business Impact: reputational damage, operational disruption

ORGANISED CRIME
Global, difficult to trace and prosecute
Motivation: financial advantage, potentially opportunistic
Business Impact: financial loss, reputational damage, operational disruption

STATE SPONSORED
Espionage and sabotage
Motivation: political and economic advantage
Business Impact: reputational damage, operational disruption, financial loss

INFORMATION

- CUSTOMER, SUPPLIER AND PERSONNEL DATA
- INTELLECTUAL PROPERTY
- COMMERCIALLY SENSITIVE INFO
- BUSINESS PROCESSES

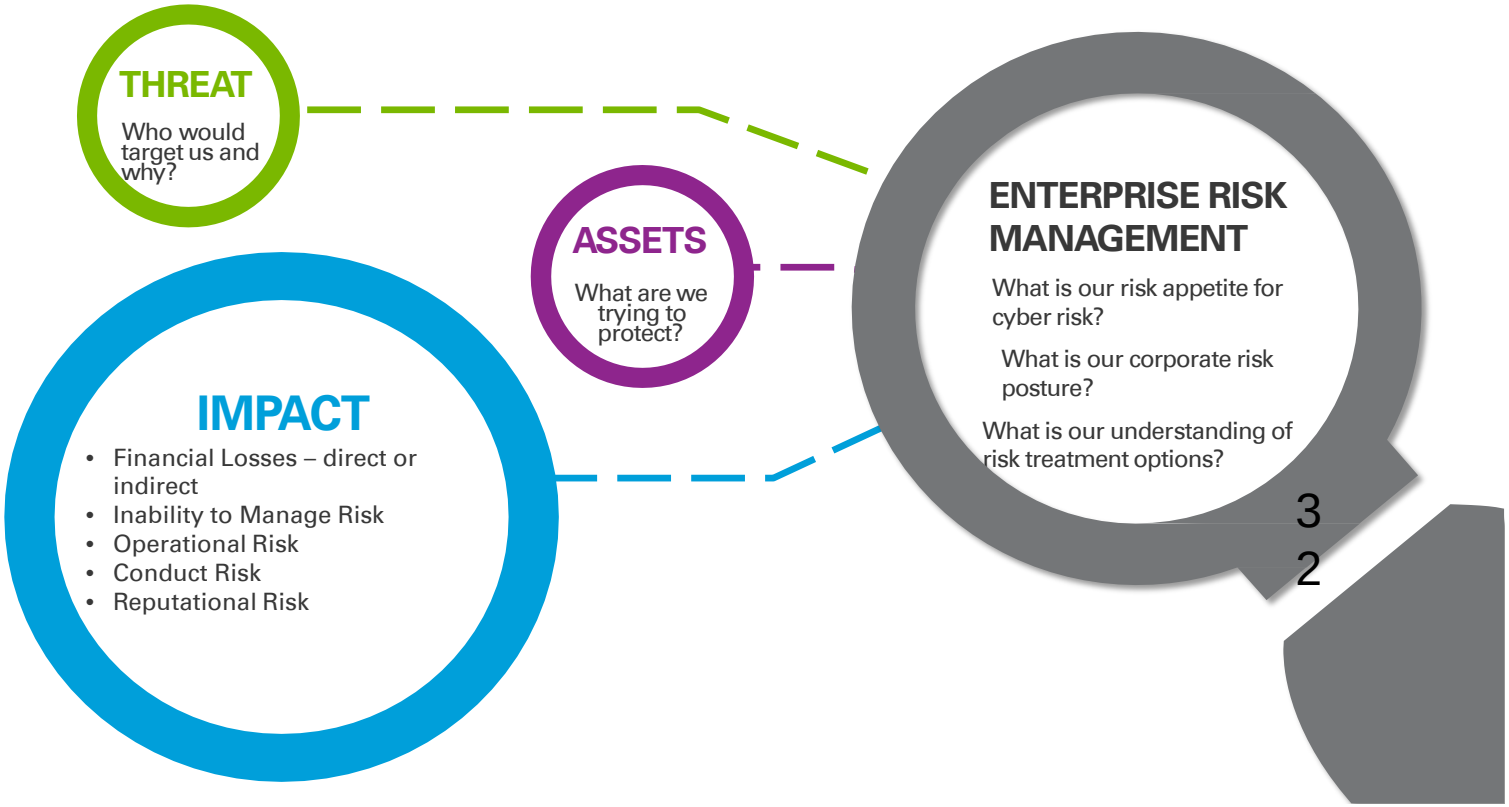
SERVICES

- CUSTOMER CHANNELS
- TREASURY / PAYMENTS FUNCTIONS
- INFRASTRUCTURE

TRANSACTIONS

- CUSTOMER INSTRUCTIONS
- B2B TRANSACTIONS E.G. INVOICING, SETTLEMENTS
- PAYMENT CARD DATA (INC. CVC)

WHAT IS BEING TARGETED?



Key Questions - Different levels

The Board

Are we a security resilient organisation?

Will future acquisitions Change our security posture

Do our long term business plans change our information security risk position?

What do our clients think about our approach to information security?

Is our information security strategy adequately mitigating the threats?

Are we taking a consistent and efficient approach to information security risk globally?

COO & CIO

Are we spending the right amount on information security?

Do we have effective governance and control in place for information security?

Do I have the right strategy?

How does our security capability compare to our peers?

Head of Information Security

Am I investing in the right improvement projects?

Do I have the right talent and skills in my team?

Defending the Realm


Know thy Crown
Jewels!


. . . but don’t forget
dependencies


Where are your
crown jewels?

Could your crown jewels be.....

- **Shared with 3rd parties?**
- **In your supplier's networks?**
- **Scattered all around the place?**

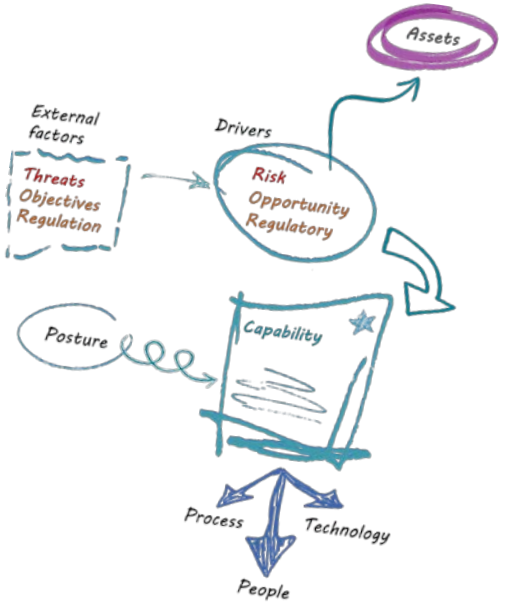

Make some plans?
THE ART OF
MILITARY
STRATEGY


Build some defences

Key things to have in modern cyber defence

- **Determination**
- **Data**
- **Knowledge base**
- **Team**
- **Money**

Response - How can these risks be mitigated



Common Mistake – The natural desire to find a technical solution to an inherently human problem leads to significant risks left unmitigated or inefficiently addressed

Getting the basics right - Cyber Essentials Scheme

Of the basic but successful cyber attacks against UK businesses and citizens of which Government has detailed knowledge, the large majority would have been mitigated by full implementation of the controls under the following, selected categories:

1. Boundary firewalls and internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

To implement these requirements, organisations will need to determine the technology in scope, review each of the five categories and apply each control specified. Where a particular control cannot be implemented for a sound business reason (e.g. is not practical or possible) alternative controls should be identified and implemented.

Source: Cyber Essentials Scheme Requirements

The Cost of Doing Business in the 21st Century

- Assume your organisation is a target.
- Assume your existing security controls can be bypassed.
- Apply the basics (patching, malware, education, leadership)
- Ensure you are able to detect and react to critical risk events quickly.
- Tap into external intelligence through providers and communities

Questions?

KPMG

Hot topics

Hot topics

As a starter . . .

EU General Data Protection Regulation (GDPR)

Hot topics - EU GDPR

Scale of fines for non-compliance - maximum fine capped at the greater of €20 million or up to 4% of total worldwide turnover.

Mandatory breach reporting within 72 hours

Requirement for Privacy Impact Assessments (PIAs)

No Safe Harbour

Required use of processors

Significant changes to consent requirements

Mandatory appointment of a Data Protection Officer (for some)

Right to erasure

Enhancement of Data Subject rights

Privacy by design

Increased security requirements

Inventory required

Requirement to register as a Data Controller likely to disappear

Mandatory Privacy policies

Increased transparency needed

Hot topics

What are your burning issues?

KPMG

Closing remarks

What next?

Are you interested in a Derbyshire Audit Forum?

If so…..

- **Would it benefit other members of your audit committee?**
- **What topics do you want to see covered?**
- **How often would you like to meet?**

But for now, thanks for coming today!

Thank you

Contacts

John Cornett
Director
KPMG, Public Sector
St Nicholas House
Nottingham, NG1 6FQ

Tel: +44 (0)116 256 6064
Mob: +44 7468 749 927

KPMG
cutting through complexity™

Contacts

Tony Crawley
Director
KPMG, Public Sector
1 Waterloo Way,
Leicester, NG1 6LP

Tel: +44 (0)116 256 6067
Mob: +44 7966 184 819

KPMG
cutting through complexity™