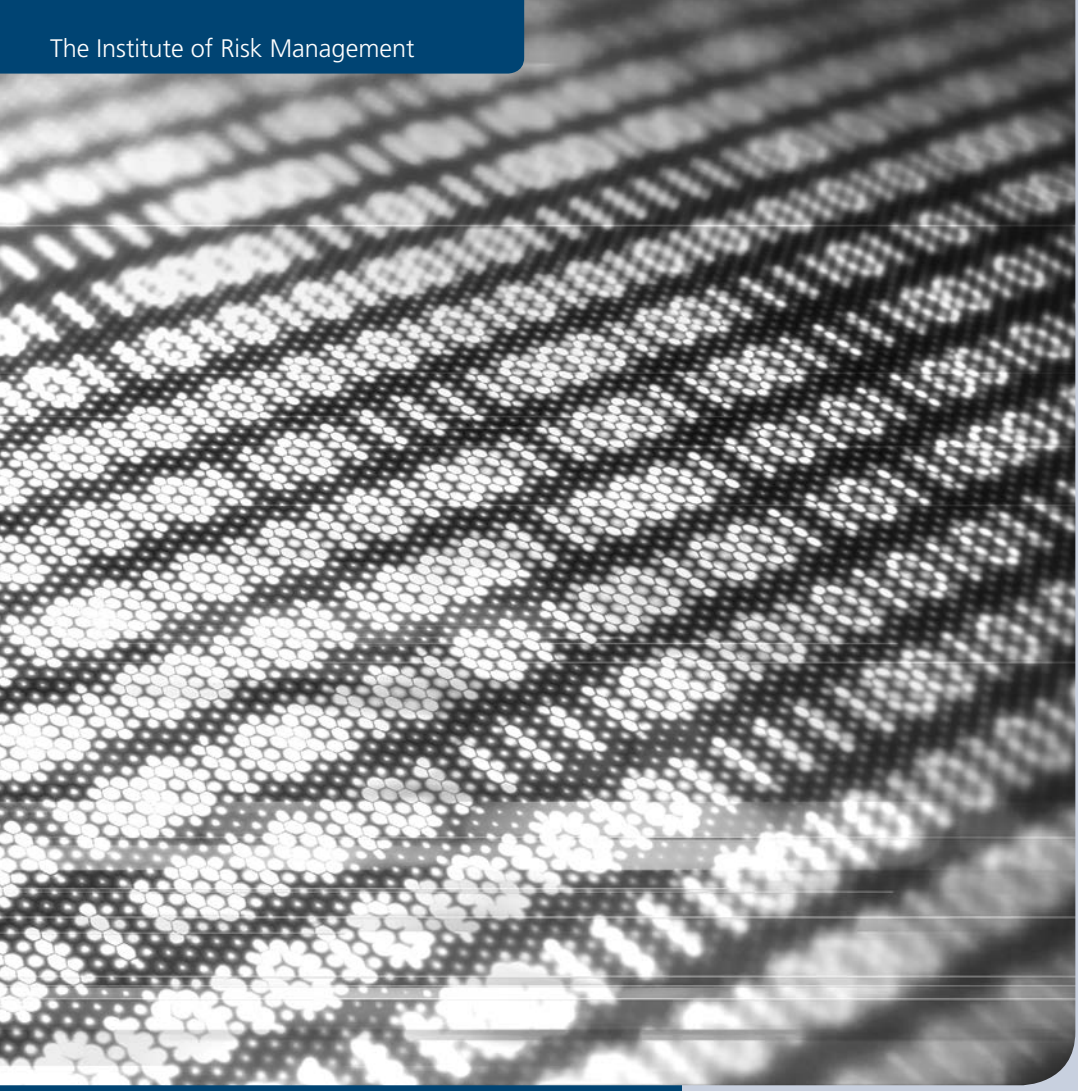
The Institute of Risk Management



Cyber Risk

Executive Summary

CGI

Experience the commitment®

irm

Leading the risk profession

Our supporters

Moving from a range to a single number risk allowance is a matter of judgement.

Contents

Who are the IRM?

This work has been led by members of the Institute of Risk Management, which for over 25 years has been providing leadership and guidance to the emerging risk management profession. In its training, qualifications and thought leadership activity, including seminars, special interest and regional groups, the Institute aims to bring together sound academic work with the practical experience of its members working in many diverse types of organisation worldwide. IRM would like to thank everyone involved in the background research and in making input to the project group working on these cyber risk guidance documents.

Foreword

Over the past twenty years our working and personal lives have been transformed by the use of technology.

I frequently say that the role of risk management is to be the disruptive intelligence that pierces the 'perfect place arrogance' so often encountered in organisations of all types. Our professional inclination to be upbeat and optimistic, together with significant personal and organisational investment in how things are, can lead to us being slow to react, or even wilfully blind, to major shifts in the risk landscape and our capabilities for dealing with them. At the same time, corporate governance developments around the world are placing explicit responsibilities on boards to ensure that they understand and manage their risk exposures.

Cyber risk is one such development. Over the past twenty years our working and personal lives have been transformed by the use of technology. We can do things now to access and organise information, and to communicate with each other, that we could not conceive of in the last century. The pace of these developments shows no sign of abating. Technology has brought us huge benefits, but it also poses risks that need to be understood and managed.

While the risks might seem new, the ways of dealing with them are now well established. The IRM has worked to develop the profession of risk management, providing education, training and practical guidance to help organisations approach their risks in a systematic and effective way, from the board down to the shop floor.

This short document summarises the work undertaken by IRM's Risk in Information Systems and E-business (RISE) special interest group (SIG). It also incorporates ideas discussed at a series of round table events organised by IRM in partnership with BAE Systems Applied Intelligence. It is relevant for all professionals, particularly for those working at board level, and we finish by offering a set of questions that all boards should ask, and be able to answer, about their organisation's management of cyber risks. It is not a technical document about computers and networks (there are plenty of those elsewhere). It is a document about risk management in the context of cyber risk, which we think is breaking new ground. There is also a longer companion document – Cyber Risk – Resources for Practitioners – which covers the detailed thinking behind the high level guidance and also offers practical tools and insight into the subject areas. This longer document is available for download to IRM members and the members of our supporting organisations from their respective websites.

As with all our thought leadership work, we are gathering together risk experts to look at fast-moving areas where practice is still being developed. We don't therefore think that what we have written here will be the last word on the subject – we expect to see new ideas and practices emerging and welcome comments.

I am grateful to the RISE SIG, and particularly to its leaders Alastair Allison, David Canham, Matt Hillyer and Dan Roberts, for the enormous amount of work they have done to bring these documents together. I would also like to thank the wider international group of practitioners, experts and associations that the SIG has brought together to produce, contribute to and comment upon this work. Thanks are also due to our sponsors CGI who have made possible the design and print of these documents as well as contributing to the content. As a not-for-profit organisation such support is invaluable in helping us maximise our investment in the development and delivery of world class risk management education and professional development.

Richard Anderson, Chairman, Institute of Risk Management

Every day the media report another organisation which has been the victim of a cyber-attack. Usually it's the loss of corporate data, intellectual property or customers' financial details – or at worst sometimes all three. The consequences have varied from regulatory fines and reputational loss, through to the complete failure of a business and we know that cyber criminals can infiltrate an organisation's systems for days, or even years, without being detected. So businesses and government need to understand where the key cyber risks exist within their organisation, how to detect them and how to protect themselves from this rising threat, at the right level of cost. CGI is delighted to support this IRM Cyber Risk document of new approaches and best practice, and we look forward to engaging with their members to help them become confident that they are successfully managing their cyber security risk.

Tim Gregory, UK President, CGI

CGI

Experience the commitment®


“
Over the past twenty years our working and personal lives have been transformed by the use of technology.”

Our project team

IRM would like to thank the following who have contributed in various ways towards the drafting and review of this guidance.

Members of the IRM RISE Special Interest Group

Alastair Allison SIRM, Zurich Insurance Group

Angeliki Chatzilia, Crowe Horwath Global Risk Consulting

David Canham, MIRM, Aviva PLC

Matt Hillyer, CIRM, TNT UK Ltd

Dan Roberts, SIRM

Harvey Seale, CIRM, Nuffield Health

Matt Willsher, BAE Systems Applied Intelligence

Carolyn Williams MIRM, Institute of Risk Management

Also with thanks to:

GCHQ

Wendy Holt, CGI

Paul Hopkins, CGI

Tim Stapleton, Zurich North America

CPNI

Roger Garrini, Selex ES

Andy Coombs, HMRC

Jennifer Wood, HMRC

Julian Phillips, JP Risk

Dorothy Maseke, UAP Kenya

Jeff Miller, Zurich Insurance Group

“Digital technologies, devices and media have brought us great benefits and offer enormous opportunities but their use also exposes us to significant risks.”

Cyber risk and risk management

We are aiming to offer some independent and practical guidance for fellow risk professionals.

Cyber risk is never a matter purely for the IT team.

Digital technologies, devices and media have brought us great benefits and offer enormous opportunities but their use also exposes us to significant risks. The media regularly present us with examples of organisations that have suffered financial loss and reputational damage as a result of problems arising from their information technology systems, whether this is as a result of human error, deliberate wrongdoing or some other form of technology systems failure. Governments and regulators are getting interested and are increasingly calling on businesses to take action to protect both their own assets and also the national infrastructure.

Those responsible for risk management within an organisation need to have a full understanding of the nature of the risks and also of the practical tools and techniques that are available to address them. Increasingly regulators and investors will expect organisations to provide information on their cyber exposures, which should be integrated with the organisation's overall consideration of risk exposure and appetite. Cyber risk is never a matter purely for the IT team (although they have an vital role) as human and organisational factors are just as important as having the right hardware and software.

This guidance document from the IRM's RISE (Risk in Information Systems and E-Business) Special Interest Group attempts to de-mystify the subject of cyber risk. We are aiming to offer some independent and practical guidance for fellow risk professionals. Other professionals outside the IT field may also find it useful. Some of the group's findings and recommendations are based on research amongst IRM members around the world. The document is intended primarily for risk professionals, from all types of organisation and in all locations, who are charged with ensuring that their own organisations are equipped to manage these risks, but there are also some important messages for the boards of organisations, where ultimate responsibility will lie. Effective governance arrangements for cyber risk issues are needed.

What do we mean by cyber risk?

Use of the cloud in itself neither increases nor decreases the risk profile.

By 'cyber risk' we mean any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

By 'cyber risk' we mean any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.

Such a risk could materialise in the following ways:

- deliberate and unauthorised breaches of security to gain access to information systems for the purposes of espionage, extortion or embarrassment.
- unintentional or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed
- operational IT risks due to poor systems integrity or other factors

Organisations should not only be concerned with these things happening to them directly, but should also consider the effects should key companies in their supply chain or other parts of their extended enterprise be affected.

Increasingly organisations will have suppliers in the new world of outsourced services and infrastructure that has been termed "the cloud". Use of the cloud in itself neither increases nor decreases the risk profile; an effectively controlled environment migrated to the cloud will, if the controls remain in place, continue to be effectively controlled, while a poorly controlled environment will be fraught with risk and threat regardless of the IT infrastructure choice.

Cyber = Opportunity

Mobile devices have become part of our everyday life.

Risk managers will need to be creative to find a balance between what the user wants and what the organisation needs.

New ways of working bring risks as well as opportunities. The business benefits offered to organisations by cloud computing, BYOD[1], social media and the 'internet of things' introduce a range of new risks as well as causing existing risks to evolve. Keeping track of this rapidly changing world while maintaining the flexibility to react to opportunities will be a challenge to organisations.

Social media has brought vast changes to our personal, social and business lives and has the potential to offer enormous opportunities or do great damage to organisations. An effective response plan to address this new environment will include the development of a social media policy, deployment of a multi-disciplinary team, effective training, careful handling of customer complaints and active monitoring of the organisation's own presence on the web.

Mobile devices have become part of our everyday life and the lines between business and personal use have become blurred, with implications for organisational security. The RISE group's research found that over 90% of respondents said that their organisations allowed the use of personal mobile devices for business use, but only 37% exercised any controls in relation to the configuration and security of these devices. Risk managers will need to be creative to find a balance between what the user wants and what the organisation needs.

1 Bring Your Own Device

"It will never happen to us"

…the average cost of a data breach to an organisation in 2013 ranged from $1.1m in India to $5.4m in the US.

Small businesses are not immune to cyber risks.

Because the risks arising from cyber activities, particularly the use of the internet, are relatively new, many organisations do not have a lot of experience in understanding or dealing with them. But the message coming to us from government and from specialist agencies is that no-one is immune. The European Commission estimates that more than one million people worldwide are the victims of cyber crime every day.[2] All types and sizes of organisations are potentially affected, not just financial services firms, defence organisations and high profile names.

According to the 2013 Annual Study: Global Cost of a Data Breach, conducted by the Ponemon Institute, the average cost of a data breach to an organisation in 2013 ranged from $1.1m in India to $5.4m in the US.

Small businesses are not immune to cyber risks – there is growing evidence that criminals are targeting the less protected organisations. Much of the advice given in this document, particularly that relating to basic precautions and controls, can be applied in a proportionate way in small businesses.

2 *Strategic Risk* Cyber Guide 2012

"So I'll go and buy some insurance"

Insurance is important but it doesn't cover everything.

Many of the risks of a security breach can be covered by insurance and this will form an important part of the cyber risk control programme. Insurance cover can include the costs of:

- forensics investigations to determine the severity and scope of a breach
- notifying individuals that they have been affected by a breach
- operating a specialist call centre to deal with enquiries from those affected
- providing free credit and identity monitoring to reassure those affected
- hiring a PR firm to provide specialist advice
- legal defence costs, settlements and indemnity payments

Insurance is important but it doesn't cover everything. Organisations will incur the costs of reputational damage, loss of customers, stock devaluation, corrective measures, IT upgrade costs and devaluation of intellectual property, the cumulative costs of which can exceed the insurable loss many times over. In many cases it is the control environment and the cultural and behavioural issues that need to be understood and addressed (and invested in) in addition to technical security measures. A coherent and business wide risk-assessment programme to understand and minimise the risks before a breach occurs is required to address the iceberg impact of a cyber-loss.

Training and investment are vital

'The carbon layer' – people – can be a weak point but is also the organisation's main asset and defence.

People – what Verizon[3] calls 'the carbon layer – can be a weak point but are also the organisation's main asset and defence. Investment in training programmes and communications campaigns can be very effective, particularly where account is taken of the organisation's risk culture and how this influences the transfer of what is learned into everyday activity in the workplace.

Basic precautions should not be taken for granted

…about **80%** of cyber attacks would be defeated by basic security controls.

It is absolutely crucial that organisations know what constitutes their data "crown jewels", be it customer data, credit card data, intellectual property or knowledge and have a clear understanding what value it brings to the organisation. According to Verizon, 99% of breaches involved techniques that were not considered highly difficult and the UK government security services maintain that about 80% of cyber attacks would be defeated by basic security controls.

Having identified the key data, organisations need to review the risks to determine potential motivations for an attack.

It is absolutely crucial that organisations know what constitutes their data "crown jewels".

3 2013 Data Breach Investigations Report, Verizon

Managing an incident

It will happen to you, so you need to have a robust incident response procedure in place.

Some form of data breach, deliberate or accidental, is now considered inevitable for all organisations at some point. It will happen to you, so you need to have a robust incident response procedure in place to minimise financial and reputational damage when a breach occurs.

Risk professionals need to make sure that their processes can respond to a breach in a timely manner to protect the organisation's reputation as well as minimise any harm to clients and customers.

Conclusion

The threats are pervasive and agile, of national and international concern and consequently, all organisations need to accurately assess the cyber risk on their organisation. We have looked at some of the key risks facing organisations and put together this document that aims to help risk professionals assess the risk by de-mystifying it.

Stripped of the 'techie speak', cyber risk is just another sort of risk which should be properly dealt with within the organisation's risk management framework and processes. We aim to bring about a sense of perspective that will allow for an informed debate, free from the scaremongering.

With the right approaches, organisations can face up to the risks and with simple controls, eradicate the majority of the threats, make cyber-crime more difficult to achieve and safely seize the huge opportunities that technology, cloud, social media and mobile devices can bring.

With the right approaches, organisations can face up to the risks and with simple controls, eradicate the majority of the threats, make cyber-crime more difficult to achieve and safely seize the huge opportunities that technology, cloud, social media and mobile devices can bring.

Questions the organisation should ask itself about cyber risk

Governance and assurance

- Do we have an effective enterprise risk management process in place and are cyber risks fully integrated into this process?
- Are we clear who is responsible for managing risks, can we identify who on the board is responsible, who explains the risks to them and on what information will decisions be made?
- Have we considered our risk appetite in relation to cyber risks, have we communicated this to all functions and do we know if our resources being deployed effectively? How would we know if inappropriate risk taking was taking place?
- Are we fully aware of the regulatory and legal exposure? What privacy and data security laws and regulations might the organisation be subject to? What are the implications for our investment decisions?
- Does our cyber-risk strategy support our wider strategic priorities? Does our risk mitigation facilitate and enable growth? Are our controls delaying or blocking progress and are we agile enough to exploit market opportunities?
- Do we invest sufficiently in cyber risk mitigation, including training, incident preparedness and assurance? How do we prioritise our investment?
- Does our culture support the necessary activities to manage this risk?
- Does our internal audit programme give us sufficient assurance in respect of our cyber risk management?

Understanding the risk

- What is the value of the information we hold (e.g. intellectual property, financial, strategic plans and other business critical information, customer/personal data)? What are our 'crown jewels' that need the most protection?
- What is the potential impact if this information is stolen or corrupted (e.g. reputational damage; damage to market value and share price; loss of competitive advantage and market share, direct liabilities to third parties affected, regulatory censure)?
- How much would it cost a third party to obtain this information and what could it be worth to them?
- What are our customers/clients' expectations of our cyber security?

Questions the organisation should ask itself about cyber risk

Understanding the risk

- How many of our critical business functions are outsourced to third parties? Have we conducted due diligence on the cyber security risks across our extended enterprise and supply chain, including the use of cloud based services? How much private and sensitive information is shared with these third parties? What provisions are there in the contracts to deal with cyber risk?
- Are our systems engineered to the best levels of security? What could be improved?
- Do we have an effective mobile device strategy? How do we control the use of personal devices for organisational business?
- Are we using social media in our organisation? How do we know what our employees, customers and the public are saying about us on social media? Do we have a social media strategy and could we manage a social media crisis?

Incident response

- How will we know if we are being or have been attacked?
- Do we have an incident response plan and have we tested it? Do we have arrangements to obtain specialist advice and services post-breach (e.g. customer help lines)?
- Who has the responsibility to declare a cyber risk incident?
- Do our business continuity plans include cyber risk scenarios?
- Might we have cover under our existing insurance policies for financial losses caused by cyber-risks? Are there any other risk transfer possibilities?
- Are we prepared to do a root cause analysis following a breach, particularly to identify human factors, and are we prepared to act on the findings?
- Could we defend our level of preparation in the aftermath of an attack?

Training

- Do we have an effective cyber risk training programme in place including reporting of breaches and subsequent actions?
- Are there initiatives in place to support learners after the training has taken place?
- Does our cyber risk training focus on the technology, the organisation or the individual?


“
Do we have an effective enterprise risk management process in place and are cyber risks fully integrated into this process?”

IRM

T: +44(0) 20 7709 9808
E: enquries@theirm.org
W: www.theirm.org

Address:
Institute of Risk Management
6 Lloyd's Avenue
London
EC3N 3AX
United Kingdom

CGI

Paul Hopkins
Cyber Security Technical Authority
paul.hopkins@cgi.com

Wendy Holt
Strategy & Innovation Director
wendy.holt@cgi.com