



INSTITUTE OF DIRECTORS
IN IRELAND

MASON
HAYES &
CURRAN



CYBER SECURITY IN THE BOARDROOM

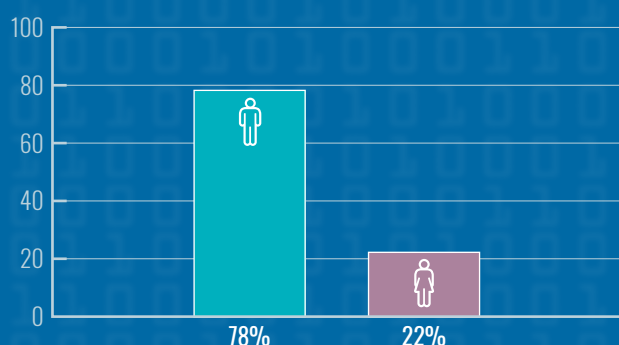
MAY 2016

For this research report, **Cyber Security in the Boardroom**, the Institute of Directors in Ireland (IoD), in partnership with Mason Hayes & Curran, surveyed 282 IoD members who are currently acting as board members in either an executive or non-executive capacity.

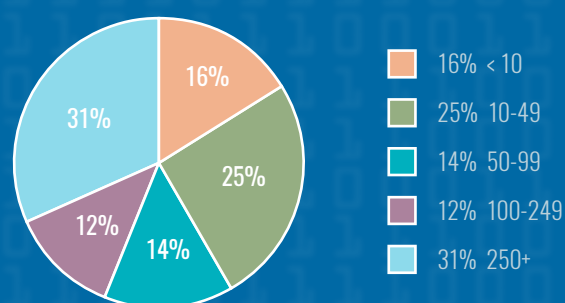
Research was conducted online between 4th - 13th April 2016.

BASE NUMBERS

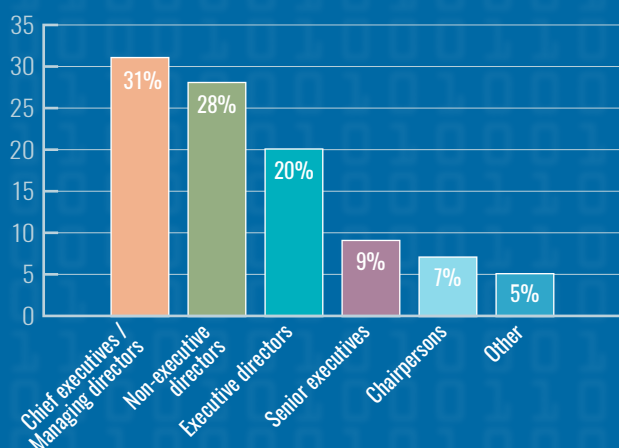
GENDER



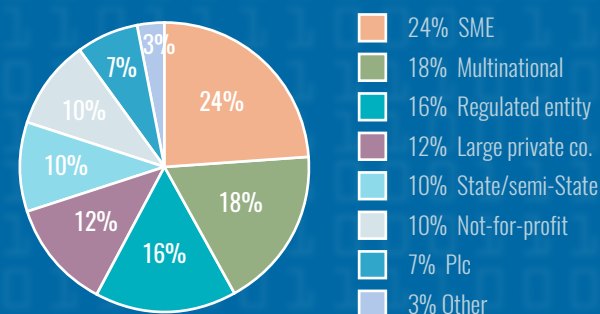
COMPANY SIZE BY NUMBER OF EMPLOYEES



POSITION



COMPANY TYPES



The Institute of Directors in Ireland (IoD) is dedicated to supporting and developing Ireland's business leaders. We are a dynamic network with 2,500 members drawn from companies large and small in the private, public and not-for-profit sectors. As the leading voice in the debate on improving corporate governance standards, our key focus is on the personal and professional development of our members with online resources, workshops, specialist courses and inspirational events. Find out more - www.iodireland.ie

Mason Hayes & Curran is an award-winning Irish law firm. Our Corporate Governance and Data Privacy teams provide an integrated and extensive range of advice on all aspects of Irish corporate compliance and data security. Our lawyers have advised on the largest data breaches in Ireland and also act as trusted counsel on pan-European data privacy issues. Our unrivalled track record ensures that we can respond rapidly to address any potential or emerging issues. Download our Cyber Security for Directors App or contact our team to find out more - dublin@mhc.ie

CONTENTS

–	Executive Summary	02
1	Is Cyber Security on the Board Agenda?	03
2	Are Ireland's Boardrooms Prepared?	04
3	Risk and Impact	05
4	Conclusions & Recommendations	07

EXECUTIVE SUMMARY

Cyber risk and security has become an important strategic concern for Irish directors and boards.

The reliance placed on information systems, both for the storage and transmission of data, is making data security breaches more damaging to organisations. It is clear that companies need to have data security policies in place that promote good information governance.

The aim of this research is to examine the perspectives of Irish directors from a range of company types and sizes on what changes they have noticed in terms of the importance of cyber security as a board level issue, their levels of preparedness should their organisation experience a cyber breach, and how at risk they feel their organisation is in terms of cyber liability.

The report also outlines the main types of breaches that have been experienced by respondents in the past, and provides a series of recommendations on how directors and boards can best prepare and protect themselves from a cyber security perspective.

Overall, there are a number of very positive findings. Respondents recognise the importance of cyber security as a board level issue and indicate a high level of preparedness should their organisation experience a serious cyber security breach. A significant majority of organisations have an identified executive with overall responsibility for cyber security issues, and the respondents themselves indicate a high level of understanding of the types of cyber risks facing their organisations.

The report also highlights areas for improvement, particularly regarding the formalisation of cyber risk issues into a formal cyber security strategy, and the frequency at which cyber security is being discussed at board meetings. Formalisation of cyber security risk issues through policies and structures

could – by focusing attention and increasing security - also contribute to a reduction in many of the most common breaches experienced by respondents, for example the loss / theft of company mobile devices, and data protection breaches, such as the inadvertent disclosure of personal data.

Techniques of cyber attack are never static, and the continuously changing face of cyber risk means that directors and boards need to keep up-to-date in their understanding of the risks facing their organisation in order to best protect against and mitigate the risks of serious security incidents.

Organisations that successfully reduce the chances of a security breach not only guard their data, but also protect their reputation, avoid potential legal liability, and reduce the potential for major business disruption and financial loss.



Maura Quinn
Chief Executive
Institute of Directors in Ireland



Paul Egan
Partner, Corporate
Mason Hayes & Curran

IS CYBER SECURITY ON THE BOARD AGENDA?

Q How would you rate cyber security in terms of its importance as an issue at board level?



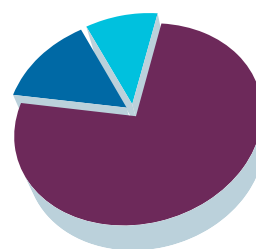
93% Very / Quite Important

Q What changes, if any, have you noticed in terms of the priority placed on cyber security at board level over the last 3 years?



41% - Significant increase in priority
35% - Moderate increase in priority
22% - No change in priority

Q How often is cyber security discussed at board meetings?



75% - At a minority of board meetings / never at board meetings
14% - At a majority of board meetings
10% - At every board meeting

There is broad consensus that cyber security is an important issue at board level for organisations in Ireland. Once seen as an issue for the IT department, cyber risk and the threat of cyber crime is now an issue that must be considered at the highest level of an organisation. And, while a significant majority of respondents have noticed an increase in the priority placed on cyber security at board level in their organisations over the last three years, interestingly, this doesn't appear to have translated in terms of its frequency as an item on the agenda at board meetings, with 75% of respondents saying that cyber security is discussed at a 'minority of' or 'never at' board meetings.

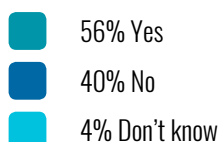
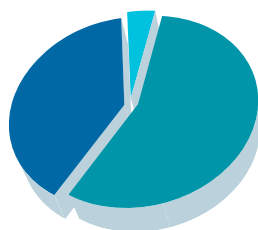
Given the serious commercial consequences arising from cyber liability, including, but not limited to, reputational damage, disruption to business, financial loss, administrative sanction and litigation / liability for damages, it is vital that cyber security is placed firmly on the board agenda, especially for organisations that deem themselves high or medium risk in terms of cyber liability.

Directors themselves also have legal responsibilities to their organisation in terms of the assessment and mitigation of risk, and this extends to cyber risk. Directors have fiduciary duties under the general law and statutory duties under data protection legislation, along with duties under several other bodies of legislation.

Additional commentary provided by respondents suggests that cyber security is being discussed at risk committees, rather than at the board itself, and while from a governance perspective it is to be encouraged that a committee, where practical, assumes delegated responsibility for more detailed focus on cyber security issues, it remains the responsibility of the board, as a whole, to be fully briefed and aware of the issues. Managing cyber risk is a concern for the entire organisation, and should be led from the top.

ARE IRELAND'S BOARDROOMS PREPARED?

Q Does your board / organisation have a formal cyber security strategy in place?



It is noteworthy that half of respondents say that there is a formal cyber security strategy in place within their organisation. Regardless of size, it would be recommended that all companies develop a cyber security strategy, the complexity of which will depend on the size and nature of the business. At a basic level, all organisations should know their information assets - whether it be a database of contacts, files associated with a specific project, financial data, or customer information records – and the risks to those assets. Organisations should also mitigate risks associated with any contractual obligations with respect to the organisation's own information and third party information.

Specified practices should also be in place to assist in detecting unauthorised activity on an organisation's networks and devices, and should identify, and keep under review, relevant best practices regarding cyber security.

It is more encouraging to see high levels of preparedness reported by respondents should a serious cyber breach occur, and that business continuity is being prioritised. This is especially important for businesses selling products and services online, which may be at risk of serious financial loss should they experience a breach to their e-commerce platform. Equally, it is encouraging to see that a significant majority of respondents say that their organisation has an identified executive with overall responsibility for cyber security issues, whether this is an executive with specific responsibility for security, i.e. Chief Security Officer / Security Director, or that responsibility forms part of the overall function of an executive, e.g. Chief Operating Officer, Head of IT.

Q Does your organisation sell products / services online?

Yes 30% No 70%

Q How would you describe your organisation's level of preparedness for a serious cyber security breach?

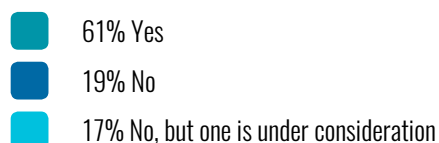
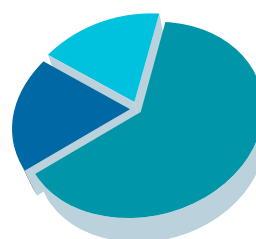
69%

28%

69% Very prepared / prepared

28% Very unprepared / unprepared

Q Does your organisation have a formal plan or strategy for responding to a cyber security incident to ensure business continuity?



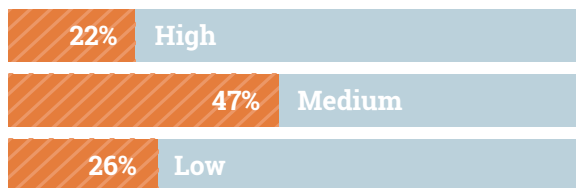
Q Does your organisation have an identified executive with overall responsibility for cyber security issues?

Yes 80%

RISK AND IMPACT

Q

How would you describe the level of your organisation's cyber liability?



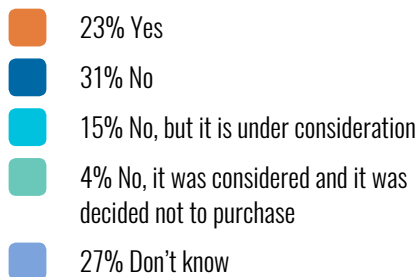
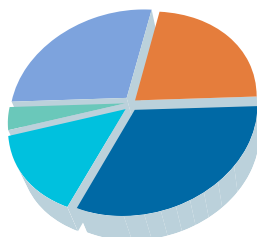
Q

How would you rate your own level of understanding of the types of cyber security risks facing your organisation?



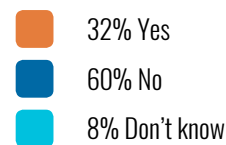
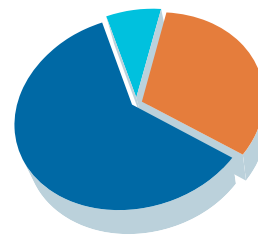
Q

Does your organisation have cyber liability insurance?

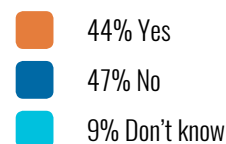


Q

Has your organisation experienced a cyber breach in the past 24 months?

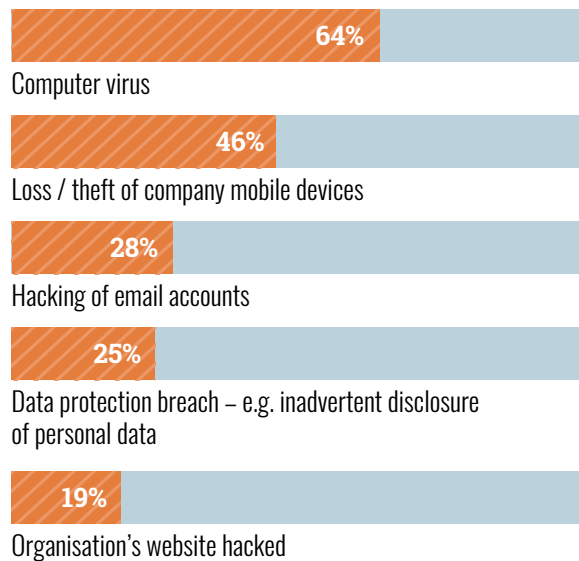


*amongst those that sell products / services online



Q

Top 5 breaches experienced by organisations



Q

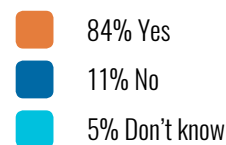
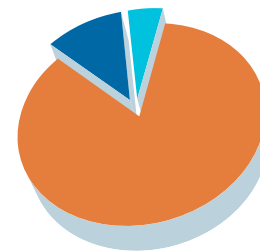
If your organisation has experienced a cyber security breach, what was the impact?

Top three impacts



Q

Do you expect that spending on cyber security protection measures will increase over the next 3 years?



Overall, one third of respondents say that their organisation has experienced a cyber breach in the past 24 months, and it is higher amongst those businesses selling products or services online. Although this is a reasonably positive finding, directors and boards should be aware that the environment is constantly changing, and as the number of computing and network services continues to grow, so too are ways and means to exploit the vulnerabilities of network devices, computer systems and applications.

Looking at the types of breaches that are being experienced by organisations, many could be mitigated with proper controls and procedures within a formal cyber security strategy, especially around the loss / theft of company mobile devices and data protection breaches, such as inadvertent disclosure of personal data.

With such a high proportion of respondents expecting spending on cyber security protection measures to increase over the next three years, it is clear that cyber security is a priority for directors and boards.

CONCLUSIONS & RECOMMENDATIONS

If you are a company director, there are a number of key questions to consider in relation to cyber security:

-  Where does cyber security fit within the company's governance framework?
-  Does the company have a cyber security strategy?
-  Do all personnel understand that there is a cyber security strategy and their role in implementing it?
-  Is the strategy understood and led from the top?
-  Has the company's cyber security strategy been tested as part of business continuity?
-  Has the company experienced any cyber security breaches in the past and what measures have been put in place as a result to protect against future breaches?
-  Do third parties pose any threat to the company's cyber security?
-  How might a breach impact on the company's reputation and what is the role of the board within that?

In answering these questions, directors should be aware that where there is a liability, there is a corresponding responsibility for that liability, and as the duties of directors and boards come under increasing scrutiny, it is in the interests of directors and boards to ensure that they have a full understanding of the cyber security issues facing their organisations and to have proper plans in place to address such risks.

It is the duty of directors, and the board, to understand, manage and mitigate cyber risk, leading from the top, and all directors should ensure that they are fully aware of their legal responsibilities in relation to cyber security.

Organisations should ensure that formal policies are in place for the management of cyber liability issues, and that appropriate structures are in place to manage and mitigate cyber liability. Such structures and policies should be subject to ongoing review, as the landscape of cyber risk continuously evolves.

It is clear that cyber security is here to stay as a key board issue, and organisations should also consider appropriate insurance policies to protect their organisations into the future.



INSTITUTE OF DIRECTORS
IN IRELAND

MASON
HAYES &
CURRAN

Institute of Directors in Ireland

Europa House
Harcourt Street
Dublin 2

Tel: +353 1 411 0010

www.iodireland.ie

Mason Hayes & Curran

South Bank House
Barrow St
Dublin 4

Tel: +353 1 614 5000

www.mhc.ie