Building Business Resilience

What the Board of Directors Need to Know
A Briefing for the C-Suite

ISACA® Central UK Chapter

ISACA® Ireland Chapter

ISACA® Northern England Chapter

ISACA® Scottish Chapter

ISACA® Winchester Chapter

Aston Business School

Cranfield University®

BREACHED OR IN CONTROL:
REVAMPING THE C-SUITE POSITION ON CYBERSECURITY

The C-level executives of all organisations no matter how large or small, whether in the private or public sectors, have a responsibility to ensure their business is resilient to the impact of adverse risks. All organisations today are reliant on technology to deliver their services to their customers and manage their business, whether they are a large financial institution, manufacturer, retailer, public sector organisation, SME etc. Indeed, many of the more successful organisations are actually technology companies, totally reliant on technology to deliver their service. Uber, Airbnb, and Amazon are just a few names which spring to mind. In our ever increasing, always connected cyber age, they are therefore exposed to the risk of a cyber-attack.

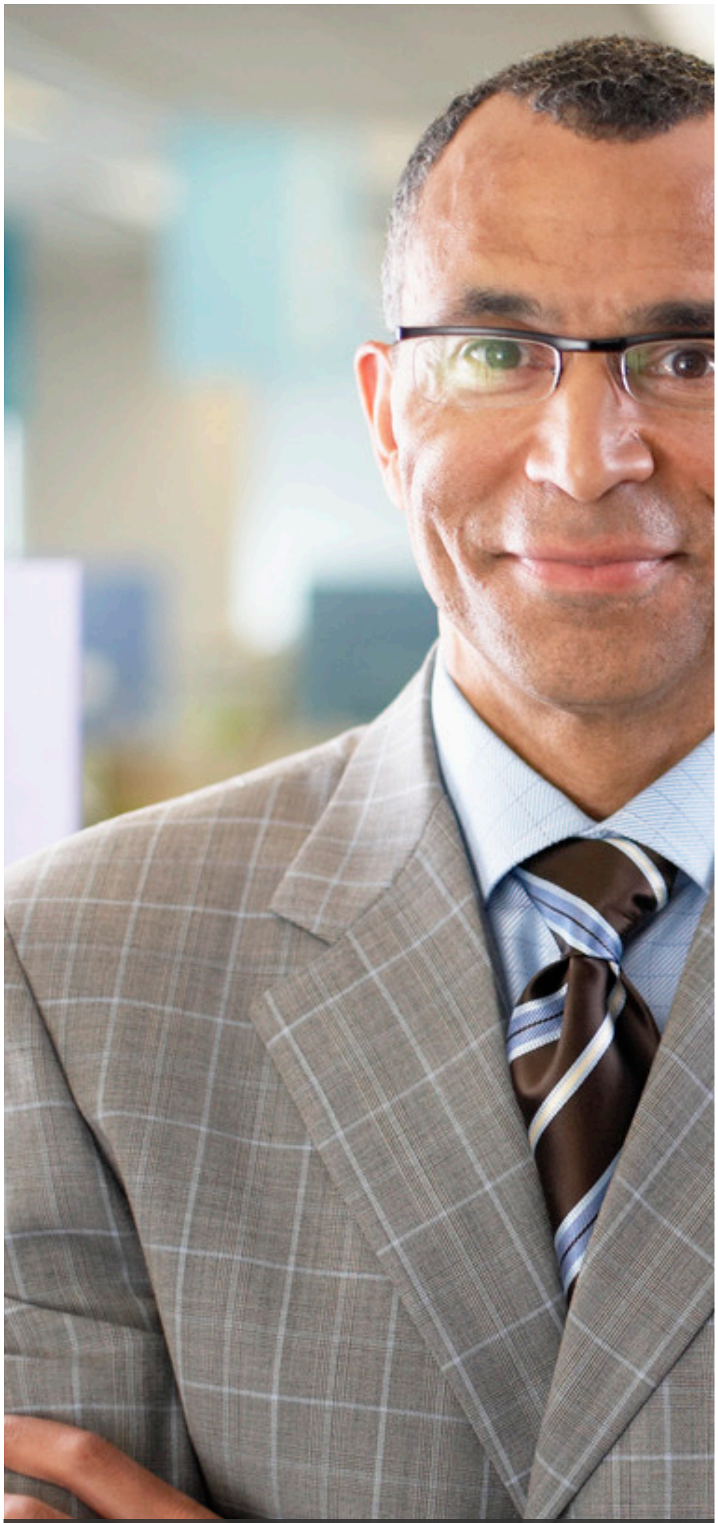
No longer can this issue be delegated to the IT senior management team, accountability rests with the C-suite, so they need to provide effective governance oversight to ensure that the business is as resilient as possible, in line with the organisation's cyber risk.

This briefing paper accompanies the ACCA's "Cyber and the CFO report". However, managing an organisation's Cyber Risk is complex and it is not just the responsibility of the CFO, it's the responsibility of the all the C-suite of an organisation. The C-level managers have to get to grips with the reality that just as they start their work day, thousands of organised crime firms wake up with the only KPI – breaking into your enterprise network.

The C-suite have many other priorities to balance, as well as the issue of the Cyber Risk. Therefore, this paper provides some guidance on the basics. The C-suite should ensure that their organisations are:

- doing the right things;
- doing them in the right way;
- doing them well; and
- protecting business value, effectively managing the cyber risk and protecting the business.

The C-suite, as company directors, have a legal responsibility to provide effective governance oversight and to ensure that the company is well managed, to protect its customers, employees, shareholders, and business partners. This extends to ensuring that the organisation fully understands their cyber risks and these are being adequately and effectively managed. The C-suite need to lead by example, not only in what they say, but more importantly, in what they do. This includes, observing the organisational security policies.



THE BOARD & THE SCOPE OF CYBER RISK

The C-suite have the potential to lead the technological advancement against cybercrime threatening their firms' financial integrity.

The cyber risk covers many aspects: data loss, business disruption and fraud, to name but three. The stark facts of financial fraud in the UK are laid bare in the UK Finance Fraud Report 2018. Just within the City of London Financial sector, cyber security innovation and technology prevented more than £1.6 billion of fraud. Is this the time to "pop the Champaign" and celebrate? Afraid not, the extent of the criminal success rates is staggering. Criminals stole £1.2 billion through fraud and scams last year within the UK.

The brutality of the challenge faced by the Financial teams worldwide in countering cyber crimes cannot be underestimated. The CFO and the C-suite can no longer hide behind technical personnel, when discharging their responsibility of preserving financial integrity of their organisation. Yet, the ACCA reports that whilst 58% report that they have "some" involvement in the management of Cyber security, only 20% have a "great deal" of involvement.

The time has come for the CFO, and their C-suite colleagues, to lead on how organisations manage cyber risks and take control of information breaches.

20%

Only 20% have a great deal of involvement in the management of their organisational cyber security

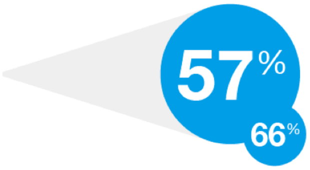
Organisations wouldn't dream of not having a business continuity plan in case of fire etc., when the probability of a fire is low, but the probability of a cyber attack is very high!

Seeking protection of the organisational financial posture through advanced security systems and innovations in which the finance industry invests to protect itself requires a degree of technical competency and a buy-in of your technical team.

The data by ACCA showed that 54% of CFOs were either not aware of whether their organisation had suffered an attack or thought that they had not been attacked at all.

However, this level of leadership requires having both a pulse on the cyberthreat landscape, which would have a major detrimental impact on the business, and the effectiveness of the organisation's cyber defences, staying ahead of evolving risks.

Recent regulatory changes have taken all executives on a data privacy and information security journey, effective cyber security being a major component. Avoiding responsibility for cyber risk by delegating, is no longer an option due, to these regulatory changes. It falls to the C-suite to take a broader view, of cybersecurity as a commercial and business-wide risk, rather than just a technical issue.



57% of CFOS ranked cybersecurity as either their most important or a 'top five' business risk. For the Financial services cyber security was ranked as a top five or higher by 66% of organisations.

Those Board Members whose organisations had been attacked, reported an immediate increase in both their awareness of the issues and their investment in countermeasures: it is clearly preferable to learn and take action before having to deal with the consequences of a security breach.

The approach to tackling these challenges will vary greatly from one organisation to another. Yet, the CFO has the overall oversight of the financial health of the organisation and therefore should be involved in the informed decision-making about cybersecurity budget in relation to the expected cybersecurity level.

According to the ACCA, while over half of respondents said they were fully aware of who had day-to-day responsibility for cyber security, 30% said they only thought they knew and 10% said they did not know.

In many organisations the IT department reports to Finance and fulfills a more supportive and operational role, so it is vital that the C-suite set the strategy and manage cyber risks effectively.

The National Cyber Security Centre (NCSC) highlights that implementing the appropriate cybersecurity processes are about effectively managing the risks of the organisation. The approach to improving and governing cybersecurity needs to be embedded as part of an organisation's overall risk management processes. It represents a continuous, and cross-departmental process, comprising of at least three components:

- establishing the cyber security baseline and identifying cyberthreats relevant to your organisation, based on risk;
- evaluation and prioritisation of cyber risks;
- implementation of effective cybersecurity countermeasures and planning organisational response to cyber incidents.

In addition, it is imperative to get the environment right. Creating a cyber security-aware culture is not something that could be achieved overnight whatever your IT budget.

Each organisation will have a different set of requirements and processes in respect to these components. However, all organisations should be able to formulate an answer to the question of: What does good cyber security management look like?

NCSC suggest that "Good cybersecurity has to work for you; it has to be appropriate to your systems, your processes, your staff, your culture and, critically, has to be appropriate for the level of risk you are willing to accept"

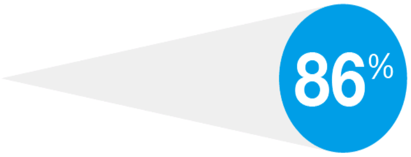
AS A BOARD MEMBER YOU ARE A PRIME TARGET

Senior executives in organisations are targets for cyber attacks due to their position, yielding access to valuable assets, both in terms of information resources and financial decision-making powers. The use of social engineering, also known as 'whaling' in the case of when C-level positions are targeted, are attacks that are low cost and yield a high success rate. Whaling exploits are sucessful, amongst other aspects, due to the reluctance of staff to challenge non-procedural requests from executives.

When it comes to cybersecurity, you need to think about your own vulnerabilities. The C-suite should consider what information is publically available that could facilitate cyber attacks based on social engineering techniques.

No longer confined to online sources, C-suite profiling by criminals can extend to the dark web where previously compromised personal and business information can be available, or offered for sale. According to ACCA only 16% identified dark web as a threat.

86% of CFOs rated their personal knowledge of cyber security as above average.



73%

73% of organisations have no cyber insurance or CFOs are not informed about it

QUANTIFYING CYBER RISK

Establishing effective cybersecurity metrics is not straightforward, as in the case of financial risk

A typical outcome of 'good' cybersecurity management is the absence of failure. The ACCA report highlights that risk of data loss, for instance, can be seen as just a privacy issue, rather than opening the organisation to other threats, such as phishing or email compromise; or alternatively seen as a financial rather than a regulatory risk.

Quantification of the cyber risk is an area where the C-suite have a crucial role in defining and quantifying the risks faced by their organisations and how they relate to their risk appetite and risk capacity. The danger of isolating cyber risks in relation to operational, financial and regulatory risks, can lead to ineffective risk management practices.

SUPPLY CHAIN

Businesses are increasingly relying on their full supply chain for to effectively deliver their business operations. According to the FTSE 350 Cyber Governance Health Check 2018, 73% of businesses recognise the risks arising from business in their supply chain, but fewer than a third (32%) acknowledge risks from 'fourth parties' that are not directly contracted to the business. As organisations continue to integrate supply chains, the recovery time after a supplier data breach and/or the resulting reputational damage, are significant factors, often adversely affecting share prices and company valuations. However, the CFO report results suggest that many do not take an active role in addressing this risk.

Supply chains are becoming more complex and the requirements imposed on SMEs by others in the supply chain, necessitate an appropriate level of cyber security protection. Constrained by the IT budgets, SMEs often view cybersecurity as a liability rather than a process essential for conducting business. Criminal networks are increasingly targeting SMEs, as they are often seen as the weakest link into a large corporate, or government body.

As with the C-suite of a corporate, the management team of an SME needs to ensure that they fully understand their cyber risks and are appropriately protecting themselves and therefore also protecting their customers and business partners, from cyber attacks. SME's have a huge challenge, protecting themselves from sophisticated cyber attacks. Keeping up with the extent of the threats can be challenging from a resource, time and a cost perspective. Maintaining an appropriate level of security for SMEs may be a matter of survival.

For a business of any size, the complexity of the interconnected organisations, some of which may be overseas, challenges the remit of cyber risk management. The traditional organisational perimeter is no longer delineated by a firewall, but rather replaced by one where authenticating the user is pivotal. The vulnerabilities may occur in the connected supply chain. The source of vulnerabilities for a business may be outside its direct control and potentially overseas. The ACCA indicated that assessments or audits of the cyber security vulnerabilities in their supply chain are patchy across organisations. Only 19% of the respondents said that they undertook these activities; which reduced to 11% for smaller organisations

Risk management practices must adopt a more proactive approach in assessing their supply chain. Auditing and advising of risk management processes are crucial, similarly to financial practices.

70% **24%**

70% of SME organisations do not undertake their supply chain audit and only 24% of large organisations REGULARLY carry out supply chain assessments.

According to ACCA organisations that still think in terms of 'perimeter security' need to think more deeply about where that perimeter is and who is guarding it.

PRACTICAL ACTIONS

As a company director, the C-suite has a responsibility to "promote the success of the company". This would include ensuring that the organisation is effectively governed and managed. The use of technology is a major enabler to business success; many organisations simply could not operate without its technology. Therefore, appropriate and effective technology/cyber governance is essential to help gain competitive advantage and ensure a resilient business. Managing your technology/cyber risk and ensuring resilience of your business is extremely complex, but if you do nothing else, then ask these key questions to ensure you are at least doing the fundamentals:

- **Do we have the basic hygiene factors in place?** *Secure configuration, including Patch Management and Malware Protection. Ensure your networked devices are configured appropriately, including no default settings. All networked devices are patched and no more than 1 month out of date. If they are on a network, they are a potential access point that can be exploited.*
- **Do we have appropriate and effective access controls?** *Implement 2 Factor Authentication, especially on Privileged Accounts and on Remote Access Users.*
- **Do we fully understand our business related technology and cyber risks?** *Fully understand your business risk of using technology and cyber-enabled solutions, and ensure that controls are working effectively to manage these risks.*

- **Are we effectively managing our full supply chain?** *Understand the risk of your complete supply chain, the risk of your third parties, and their third parties, from the perspective of the value and sensitivity of the information they handle on your behalf, and also how the supplier impacts on your organisation delivering services to your customers.*
- **Have we the appropriate security culture?** *Leadership, encouraging a technology and cyber security aware culture, including providing an ongoing awareness and education programme. The C-suite and senior management team not only saying the right things, but also backing their words, with their actions.*

- **Can we respond to incidents quickly and effectively?** *Establishing an appropriate and responsive Incident Management Capability. Recognise that breaches will happen, be prepared to Respond and Recover. Breaches will happen, you will be judged by your shareholders, regulators, customers and business partners on how well and quickly you are able to Respond and Recover.*

- **How do we know we are effective?** *Performance monitoring, defining appropriate, meaningful and easily obtainable KPIs (Key Performance Indicators) and KRIs (Key Risk Indicators). Providing easy to understand Dashboard to the C-Suite.*
- **Do we have the rights skills, in the right numbers, in the right places?** *Ensure that the* organisation has the *right cyber security skills in the right numbers; in the right places and that their training is kept up to date.*

Cyber is not an issue just for the IT senior management team, it is an organisation-wide and a business resilience issue. Cybersecurity incidents carry significant business and financial implications for the entire organisation. Cybersecurity, **ultimately**, is the responsibility of the C-suite. The C-suite should therefore give direction and leadership and provide effective governance oversight, ensuring that cybersecurity is embedded into the organisation's culture, business objectives and risk management practices. This requires a positive cyber risk culture, necessary investment decisions and the management of the cyber risk as an organisation-wide priority.

FURTHER RESOURCES

There are a number of resources to support you along this challenging journey. Here are some of the tools and guidelines, which may be of some assistance, helping the C-suite to discharge their director responsibilities.

ISACA Resources

ISACA is an independent, non-for-profit, global professional association, with a focus on technology and cyber governance, risk management, and security, engaging in the development, adoption and use of globally accepted, industry-leading knowledge ISACA has over 420,000 engaged constituents, in over 180 countries working in the areas of technology governance, risk management, assurance, and cyber and information security. ISACA in the UK and Ireland has been established for over 35 years and has over 6,500 members in six Chapters: Central UK, Ireland, London, Northern England, Scotland and Winchester.

- Business Model for Information Security
- Building a Information Security Culture
- CMMI Cyber Security Maturity Assessment
- COBIT 2019
- CSX Training Platform
- CSX Cyber Knowledge resources
- CSX Fundamentals
- CSX Foundation
- CSX Practitioner
- CISM (Certified Information Security Manager)
- CRISC (Certified in Risk and Information Systems Controls)

Other Sources

- NCSC Ten Steps to Cyber Security
- NCSC Products & Services, including Cyber Essentials.
- Cyber Information Sharing Partnership (CiSP)
- ISO 27001 and 27002
- NIST Cyber Security Framework

Bibliography:

Callaham, J. (2019), 'What is Google Duplex and How Do You Use It?' [website article] <https://www.androidauthority.com/what-is-google-duplex-869476/>, accessed 8 May 2019.
HM Government (2019), 'FTSE 350 Cyber Governance Health Check' [website article] <https://www.gov.uk/government/publications/cyber-governance-health-check-2018>, accessed 8 May 2019.
McAlaney, J., Frumkin, L., and Benson, V (eds.) (2018) Psychological and Behavioral Examinations in Cyber Security, Hershey: IGI Global.p.320 DOI: 10.4018/978-1-5225-4053-3.
NCSC Board Toolkit (2018), 'Guidance Board Toolkit, NCSC [website article] <https://www.ncsc.gov.uk/collection/board-toolkit> accessed 8 May 2019.
UK Finance (2019), 'Protecting Customers and Stopping Fraud', Dedicated Card and Payment Crime Unit. [website article] https://www.ukfinance.org.uk/system/files/Fraud%20Prevention%20Timeline%20-%20FINAL.pdf accessed 8 May 2019.
UK Finance Fraud Facts(2019), The Definitive Overview of Payment Industry Fraud', UK Finance [website article] <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf>

CONTRIBUTORS

Professor Vladlena Benson, Cybersecurity and Innovation Cluster, Birmingham, UK
Michael Hughes, Director ISACA Central UK, Partner Haines Watts and NED CyberQ group.

ACKNOWLEDGEMENTS

Dr Ruth Massie, Cranfield University, Bedfordshire, UK
Jonathan Evans, President ISACA Central UK
Feargal O'Neil, President ISACA Ireland
John Jones, President ISACA Northern England
Alison McAlroy, President ISACA Scotland
Alex Krupa, President ISACA Winchester