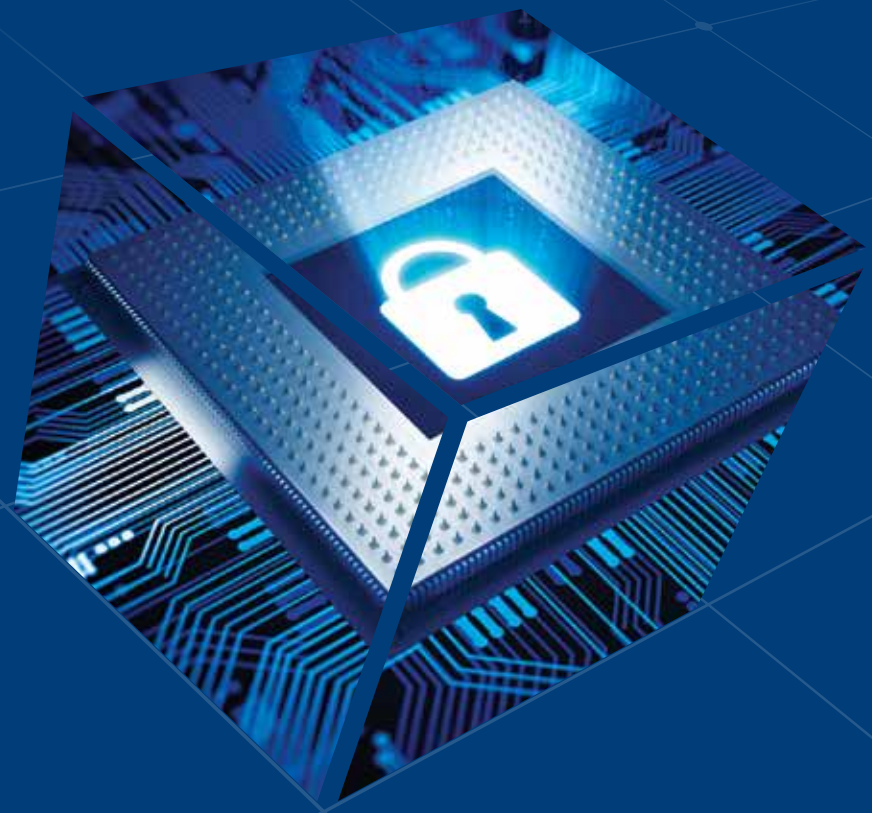
Cyber Security

What Boards Need to Know



ODGERS BERNDTSON

Search Intelligence

Executive Summary

Maintaining firewalls, protecting servers and filtering malicious emails rarely make it onto the board agenda: these issues tend to be delegated to the company's IT security experts.

But in the face of continuous and increasingly complex cyber attacks, boards of directors are under growing pressure to pay closer attention to cyber security.

Cyber attacks are becoming ever more sophisticated, as well as more frequent. Cloud computing, the proliferation of 'big data' and the growing use of mobile devices, tablets and social media are creating new and significant security challenges.

The impact can be far-reaching. Recent high profile incidents show that cyber attacks can not only strike a company's financial performance, but also inflict unquantifiable reputational damage.

No-one is immune: large and small companies, governments and individuals are all at risk.

As a result, boards are being called upon to address cyber risk alongside other risks facing the business. Directors are taking steps to increase their awareness and understanding of cyber security, and are starting to take a strategic view of its potential impact on business performance.

This paper looks at cyber security's elevation to the boardroom. It considers the nature of the threat faced by business and offers practical advice on what board directors need to know.

The traditional approach to cyber security, driven by the chief technology officer and the chief information security officer, is only part of the solution – robust cyber security also requires the direct attention of the board of directors.

Who's at risk?

Cyber crime is one of the top threats facing businesses, according to the World Economic Forum's 2013 Risk Report.

It is regarded as a "digital wildfire" sitting "at the centre of a constellation of technological and geopolitical risks" and has the potential to "wreak havoc" in the real world. It is no surprise, then, that the UK government rated cyber crime a Tier 1 threat in its 2010 National Security Strategy, and has set aside £650 million to tackle it.

The business world, too, is waking up to the cyber threat. It is a sign of the times that nearly half the 293 graduates recruited by FTSE100 defence business BAE in 2013 will join its cyber and security division, Detica.

No sector is immune to a cyber attack. Business services providers such as LinkedIn, financial services firms including Citigroup and the internet giant Yahoo have all suffered large security breaches in recent years. In September 2013, Tom Leighton, CEO of Akamai, which delivers nearly a third of global web content, said 74% of US companies experienced one or more cyber attacks in the last year.

And it's not just big businesses that are being targeted. Research by Hiscox has found that one in ten small businesses in the UK have experienced a data hack. Smaller firms are targeted not only for their own data, but also as a way of accessing larger businesses further along the supply chain.

Baroness Neville-Jones, a former Minister for Security, warns that many businesses don't even realise that their intellectual property has been stolen. "They usually have to be told about it by a third party. The level of awareness is nothing like it needs to be," she says.

In the case of one quoted online gaming business, it took two months to discover that more than 3.1 million account names and 90,000 usernames with bank details had been stolen in 2010.

Who's responsible?

Cyber criminals come in all shapes and sizes. The UK government's *Guidance for Business*, launched in September 2012 to raise awareness of cyber security at board level, identifies:

- Industrial competitors and foreign intelligence services interested in gaining an economic advantage for their own companies or countries;
- Hackers who find interfering with computer systems an enjoyable challenge;
- Hacktivists who attack companies for political or ideological motives;
- Employees or others who abuse their legitimate access, by accident or deliberately.

What's the cost?

Cyber crime is a multi-billion dollar industry. A 2011 Cabinet Office report estimates that cyber crime costs the UK £27 billion annually – £2.2 billion of this to government, £3.1 billion to individuals via fraud and ID theft, and by far the largest portion – £21 billion – to industry, in the form of theft of confidential data.

Most boards' immediate concern is the financial implications of losing customer information or other commercially sensitive material. A security breach on Sony's PlayStation Network in April 2011, in which

Cyber security is beyond many board directors' personal experience. It is viewed as an exotic, arcane and deeply inaccessible area

Most boards' immediate concern is the financial implications of losing customer information or other commercially sensitive material

hackers stole the credit card information of more than 12 million account holders, is estimated to have cost the Japanese consumer electronics group $170 million. There is also the cost of valuable intellectual property being stolen. Between November 2008 and March 2009, an employee of Valspar Corporation unlawfully downloaded proprietary paint formulas valued at $20 million, which he intended to take to a new company, worth about one-eighth of Valspar's profits that year.

Reputational damage, however, can be the biggest cost: it is impossible to quantify the long-term damage to a business's public perception following a cyber attack. Research shows that consumer trust, once lost, is very difficult to regain.

Boards will also want to focus on investors, regulators, insurers and potential litigants – all of whom are increasingly alert to cyber threats and companies' responses.

Exotic, arcane and deeply inaccessible?

Many directors are not fully aware of how technological changes are creating new and significant security challenges for their businesses.

An influential report by the Cyber Security Research Centre at Carnegie Mellon University suggests that boards are not undertaking basic oversight activities such as "reviewing budgets, security programme assessment and receiving regular reports on breaches and IT risks".

Dr Stephen Page, an experienced non-executive director and advisor on digital leadership in the boardroom, says that historically technology has only come before the board when specific issues needed addressing.

"The whole concept of having an adversary who is working in the shadows is alien to some board members. That someone would target corporate information – often for the simple reason that it could be targeted – is difficult for many to comprehend," he explains.

It doesn't help that many current board directors have spent most of their careers in a pre-internet world. "Cyber security is beyond many board directors' personal experience. It is viewed as an exotic, arcane and deeply inaccessible area," observes Dr Duncan Hine, a Fellow at the Cyber Security Institute at Warwick University and a cyber security adviser to several global firms.

Cyber attack? What cyber attack?

A lack of public information intensifies the problem. Despite the enormous cost to business, breaches of cyber security are rarely publicly reported.

In early 2009, Coca-Cola chose not to inform shareholders about a security breach which reportedly derailed its $2 billion takeover of a Chinese juice group. Even amongst chief executives, the subject seems to be taboo: not one participated in the panel debates on cyber security at this year's Davos conference.

The *Financial Times'* Gillian Tett says that the wall of silence is the result of an "agency dilemma" in the upper echelons of management: businesses are unwilling to talk openly about attacks and the associated costs for fear of being stigmatised or sparking panic.

This not only makes it hard to understand the scale and cost of cyber crime, but it complicates efforts to share best practice and increase cyber awareness at board level.

Prevention is better than cure

According to the US's National Security Agency, 80% of cyber attacks could be prevented by basic best practice. Boards can put a lock on the company's virtual front door by making sure that employees remain fully aware of cyber risks.

Policies covering secure use of the organisation's systems and information – such as restricting the use of portable media and content downloadable from the internet – should be put in place, supported by staff training on digital do's and don'ts.

A further solution is to invite individuals to test your systems and products for security vulnerabilities. Several companies including Facebook, PayPal and Samsung have created reward programs which incentivise internet users to report security flaws in return for monetary compensation.

Those closely involved with a company, but beyond its walls, should not be overlooked. Non-executive directors, for example, work primarily off-site with high level and often confidential corporate information stored on a range of mobile devices which, unlike those used by employees, are typically not protected.

Supply chain and professional service providers can also put sensitive information at risk. In October 2012, NASDAQ halted trading in Google shares when Google's financial printers prematurely released their earnings report. The leak, combined with the weak results it contained, wiped $22 billion off Google's market value.

Taking responsibility at Board level

Boards must put cyber risks firmly on their risk registers. Only 49 FTSE 100 companies list cyber security as a material risk to their business in their annual report, according to a Trustwave survey.

"Board directors are very mature in understanding risk management around physical or financial aspects, but much less so when it comes to information risk management," says Hine.

Directors are responsible for identifying the risks to their key information assets and assessing the likely impact if those assets were compromised. As one FTSE 100 audit chair told us: "It's the board's job to identify the information assets that are of the greatest value; it's the board's job to establish structures and capabilities that mitigate the risks to these assets; and it's the board's job to build an organisational culture in which everyone is aware of his or her cyber responsibilities."

However, not every risk can – or should – be mitigated. Stuart Aston, Chief Security Officer of Microsoft UK, says: "The key question is: what is an acceptable degree of loss? Boards do not have the resources or the time to protect everything and ultimately must prioritise certain information assets over others."

Without risk, there is no reward. Risk is an essential part of any business: the challenge is to balance business risk with technological safety. Historically these areas have been the responsibility of the board and IT experts, respectively.

Boards have had 20 years experience of treating IT as an operational matter, best left outside the boardroom. That is no longer appropriate

The key question is: what is an acceptable degree of loss? Boards do not have the resources or the time to protect everything and ultimately must prioritise certain information assets over others

But now business innovation and risk must come together at the board table, says Page: "To lead a business in the digital age, boards must shape their products, services and business structure with a close eye on cyber threats and risks."

Boards should be sure they understand how technical risks map on to the real world and so appreciate the implications for reputation and market value.

Working with the CTO and the CISO

Technology experts can help directors understand and prioritise the cyber risks facing the organisation and agree its most appropriate line of defence.

Regular dialogue between directors and the CTO and the CISO is essential, but should inform board discussion, rather than being seen as an end in itself.

As Hine makes clear: "Inviting the CISO to present at board meetings will help directors better understand cyber threats to the business and the actors behind them, but it's not the answer to getting a handle on cyber risk management and really controlling the risk."

By having regular conversations on how the company's cyber security strategy links into the overall business strategy, chairs will find it easier to translate IT risks into corporate risks and to communicate these risks to the wider board.

A further consideration is contingency planning. Once a breach has been discovered, early response is often critical to preventing further damage. It is the board's job to work with the CTO and the CISO to ensure the business as a whole is ready for the operational and reputational impact of a successful large-scale attack.

Governance in practice

Cyber security falls primarily to the audit committee as part of its risk management oversight, although not all audit committees have the time or the skills to keep abreast of the rapidly expanding array of cyber threats.

One solution for particularly 'at risk' companies is to create a special purpose governance entity. Page says: "It could be led by a non-executive director and reported into by senior security and technology executives within the business. This would give the board a formal, centralised place to direct technology and information management concerns while ensuring sufficient coverage of cyber risk at board level."

Another solution is to ensure that the board has access to the necessary specific expertise, whether in the form of an independent consultant or indeed as a non-executive director.

Page says: "Boards operate in a digital age and their composition should reflect this. While appointing a technology savvy non-executive could offer benefits in terms of their individual experience, the real benefit lies in their ability to help the wider board understand and assess cyber risks, navigating the difficult balance between digital innovation and risk avoidance."

A fundamental problem with cyber security (and managing technology in general) is the lack of a common language. Page says: "Boards have had 20 years experience of treating IT as an operational matter, best left outside the boardroom. That is no

longer appropriate. It is now critical to pull the right business risks out of the technical fog and for boards to reclaim ownership of digital risks and opportunities."

Companies must recruit technical people who will think like business people – or vice versa – to ensure the board can truly understand and lead in the digital age.

Asking the right questions

The UK government's *Guidance for Business* provides a list of questions designed to drive cyber risk discussions in the boardroom:

1. How confident are we that our company's most important information is being properly managed, and is safe from cyber threats?

2. Are we clear that the Board are likely to be key targets?

3. Do we have a full and accurate picture of:

   - the impact on our company's reputation, share price or existence if sensitive internal or customer information held by the company were to be lost or stolen?
   - the impact on the business if our online services were disrupted for a short or sustained period?

4. Do we receive regular intelligence from the Chief Information Officer/Head of Security on who may be targeting our company, their methods and their motivations?

5. Do we encourage our technical staff to enter into information sharing exchanges with other companies in our sector and/or across the economy in order to benchmark, learn from others and help identify emerging threats?

6. Are we confident that:

   - we have identified our key information assets and thoroughly assessed their vulnerability to attack?
   - responsibility for the cyber risk has been allocated appropriately? Is it on the risk register?
   - we have a written information security policy in place, which is championed by us and supported through regular staff training? Are we confident the entire workforce understands and follows it?

Conclusion

In the past, if you asked a company chair what kept them awake at night, few would have mentioned the challenge of securing corporate intellectual property assets and customer data, or managing the risk of sensitive commercial information being compromised.

In today's environment, however, where 90% of the world's data has been created in the last two years alone, cyber crime presents a serious threat.

Faced with intensifying and highly sophisticated cyber attacks, boards of directors are under mounting pressure to treat cyber security as a key business risk.

Boards have a crucial role to play in considering the types of attacks their company may be facing, and the financial, operational and reputational implications of a security breach.

They are also responsible for making sure their companies adopt an integrated, business-led approach to cyber security, working closely with senior IT executives to ensure that the company's security infrastructure is robust and fit-for-purpose.

Cyber security starts in the boardroom.

Further resources

"Cyber risk management: a board level responsibility" – a Department for Business, Innovation & Skills policy paper which provides an overview of the benefits of cyber risk management for senior executives (2013)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf

"10 steps to cyber security: executive companion" – a Department for Business, Innovation & Skills policy paper which offers guidance for business on how to make the UK's networks more resilient and protect key information assets (2013)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

"10 steps to cyber security: advice sheets" – a Department for Business, Innovation & Skills policy paper which provides detailed cyber security information and advice for 10 critical areas, covering both technical and cultural areas (2013)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73129/12-1121-10-steps-to-cyber-security-advice-sheets.pdf

"The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world" – a UK government policy paper which sets out how the UK supports and protects the nations cyber security (2011)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

"Partnering for Cyber Resilience" – the World Economic Forum's global initiative to improve cyber resilience and raise business standards (the UK is a member). It offers business tools to evaluate and improve their capabilities (2013)
http://www.weforum.org/issues/partnering-cyber-resilience-pcr

Websites

Cyber Incident Response – a scheme launched by GCHQ which helps companies in dealing with a cyber attack
http://www.cesg.gov.uk/servicecatalogue/cir/Pages/Cyber-Incident-Response.aspx

The Centre for the Protection of National Infrastructure – the United Kingdom government body which provides protective security advice to businesses and organisations across the national infrastructure
http://www.cpni.gov.uk/Templates/CPNI/pages/Default.aspx

Action Fraud – the UK's national 24/7 fraud and cyber crime reporting centre
http://www.actionfraud.police.uk/

Organisation for Security and Co-Operation in Europe – the world's largest security-oriented intergovernmental organisation
http://www.osce.org/

Our People

Virginia Bottomley

Virginia chairs the Odgers Berndtson Board Practice. The Board Practice conducts searches for chairs, chief executives and non-executive directors for plcs and private companies.
virginia.bottomley@odgersberndtson.com

Kit Bingham

Kit is Partner and Head of the Chair & Non-Executive Director Practice. He joined after a career in financial journalism and financial public relations. He is a member of the Business Committee of Policy Exchange, the think-tank.
kit.bingham@odgersberndtson.com

Clare Glackin

Clare Glackin is a Consultant and member of the Energy, Manufacturing and Infrastructure (EMI) Practice. Her focus is on director and senior level executive appointments in general, commercial and operational management for the Aerospace, Defence & Security sectors·
clare.glackin@odgersberndtson.com

Caroline Sands

Caroline Sands is a Principal within the CIO & CTO Practice and a member of the Technology, Entertainment & Communications Practice. She focuses on senior strategic IT management appointments.
caroline.sands@odgersberndtson.com

Contact Details

20 Cannon Street, London, EC4M 6XD
Tel: +44 20 7259 1111

Global Offices

International Executive Search and Assessment in 30 countries across the world

Americas

Brazil	Sao Paulo
Canada	Calgary
	Halifax
	Montreal
	Ottawa
	Toronto
	Vancouver
Peru	Lima
United States	Boston
	Chicago
	Dallas
	New York
	Philadelphia
	San Francisco

Europe

Austria	Vienna
Belgium	Brussels
Denmark	Copenhagen
Finland	Helsinki
France	Paris
	Lyon
Germany	Frankfurt
	Hamburg
	Munich
Italy	Milan
	Rome
Netherlands	Amsterdam
Norway	Oslo
Poland	Warsaw
Portugal	Lisbon
Russia	Moscow
Slovenia	Ljubljana
Spain	Madrid
	Barcelona
Sweden	Stockholm
Switzerland	Zurich
Turkey	Istanbul
United Kingdom	London
	Aberdeen
	Birmingham
	Cardiff
	Edinburgh
	Glasgow
	Leeds
	Manchester

Africa, ME & Asia Pac

Australia	Sydney
China	Hong Kong
	Shanghai
	Beijing
Japan	Tokyo
South Africa	Cape Town
	Johannesburg
India	New Delhi
Singapore	Singapore
United Arab Emirates	Dubai
Vietnam	Ho Chi Minh City

ODGERS BERNDTSON
Search Intelligence