NB : BOARD PAPERS

Cybersecurity: How Should Boards Respond?

April 2015

NB • NORMAN BROADBENT

COMPETITIVE EXCELLENCE THROUGH PEOPLE

www.normanbroadbent.com

THE POWER OF THE NEW CIO

Executive Summary

As businesses evolve, technology plays an increasingly significant role in the organisation. Boards not only need to ask the right questions, but also take advantage of technology and use it as an opportunity for growth. Cybersecurity needs to become an issue CEOs know about and not just read about in the Financial Times and say 'cybersecurity is managed by my IT department.' Boards have a fundamentally equal role to play in planning for attacks to the business and crucially, the financial, operational and reputational implications of such a security breach. The CIO should play an important role as the strategic advisor around the technology implications at board level and in return the CIO must grasp the broader business strategy and articulate risk from a business perspective.

Introduction

"There are only two types of companies: those that have been hacked and those that will be."
Robert Mueller, FBI Director

In 2014, we witnessed a surge in the number of increasingly complex and sophisticated cyber-attacks across all industries, in large corporates, SMEs and start-ups. The scale is staggering: last year in the UK alone, cyber criminals compromised more than a billion data records in over 1500 breaches. The cost of rectifying these breaches is escalating: last year the average cost-to-company of a data breach was £2.5m, up 15% from 2013 . It is also critical to recognise the effect that these incidents have on consumers; many of those that bank and shop online suffered the loss of their personal and financial data.

Cybersecurity has moved far beyond an issue that can simply be resolved by expensive outsourcing or more investment in software or technology. Today's cyber-attacks are complex, virtually undetectable, not constrained spatially or temporally and are driven by individuals and organisations that are resilient, persistent and able to innovate faster than their targets. The consequences can be devastating, often resulting in brand damage, loss of revenue and substantial fines.

Faced with this reality, boards are under increasing pressure to address cyber risk as a fundamental priority aligned to the wider business strategy. How should the cyber agenda, often regarded as complex and deeply technical, become a whole-of-company responsibility driven at board level?

1 Deloitte (2014) Cyber Security: Empowering the CIO

Cyber: The What, Why and How?

"It is clear that cyber-crime has a real and detrimental impact on the global economy. Over time, cyber-crime has become a growth industry; the returns are great, and the risks are low."
Raj Samani, EMEA Chief Technology Officer, McAfee

As businesses grow, technology is no longer seen as a support function, instead it is the life-blood of the company; the new 'mail room' where the highly sensitive company assets are kept. Cybersecurity is the strategies, processes and people that protect and respond to threats to these assets.

Cyber criminals take many forms, ranging from foreign intelligence services and industrial competitors to individual hackers, ideological 'hacktivist' groups and terrorists. The motivations behind these attacks are varied: financial gain, brand damage, and some crimes are simply committed for no other reason but that it is simply possible. Other threats such as human error, often stemming from company employees themselves, are not generally malicious but can be just as dangerous.

There are four basic parts to a cyber-attack:

1. **Reconnaissance:** gathering information
2. **Exploitation:** identifying the weak areas that are open to manipulation
3. **Access:** gaining entry to a network or system
4. **Goal:** leveraging weaknesses to cause damage and disruption before covering tracks

A computer virus is the most common form of attack. Access can be gained remotely; spread through a network of computers, or proximately; by directly tampering with the technology in situ. Other common forms of attack include denial of service; overloading an area of a system rendering it inaccessible; phishing; an email sent with to induce recipients to reveal their personal data, and backdoors; remotely securing access to a system and installing or modifying existing programmes.

What does this all mean? We have established that these attacks come through the electronic or digital world and the ultimate target at stake is available data. The fundamental issue here is who can gain access to this data? The word 'cyber' is arguably a red herring; the issues facing companies are issues of data protection.

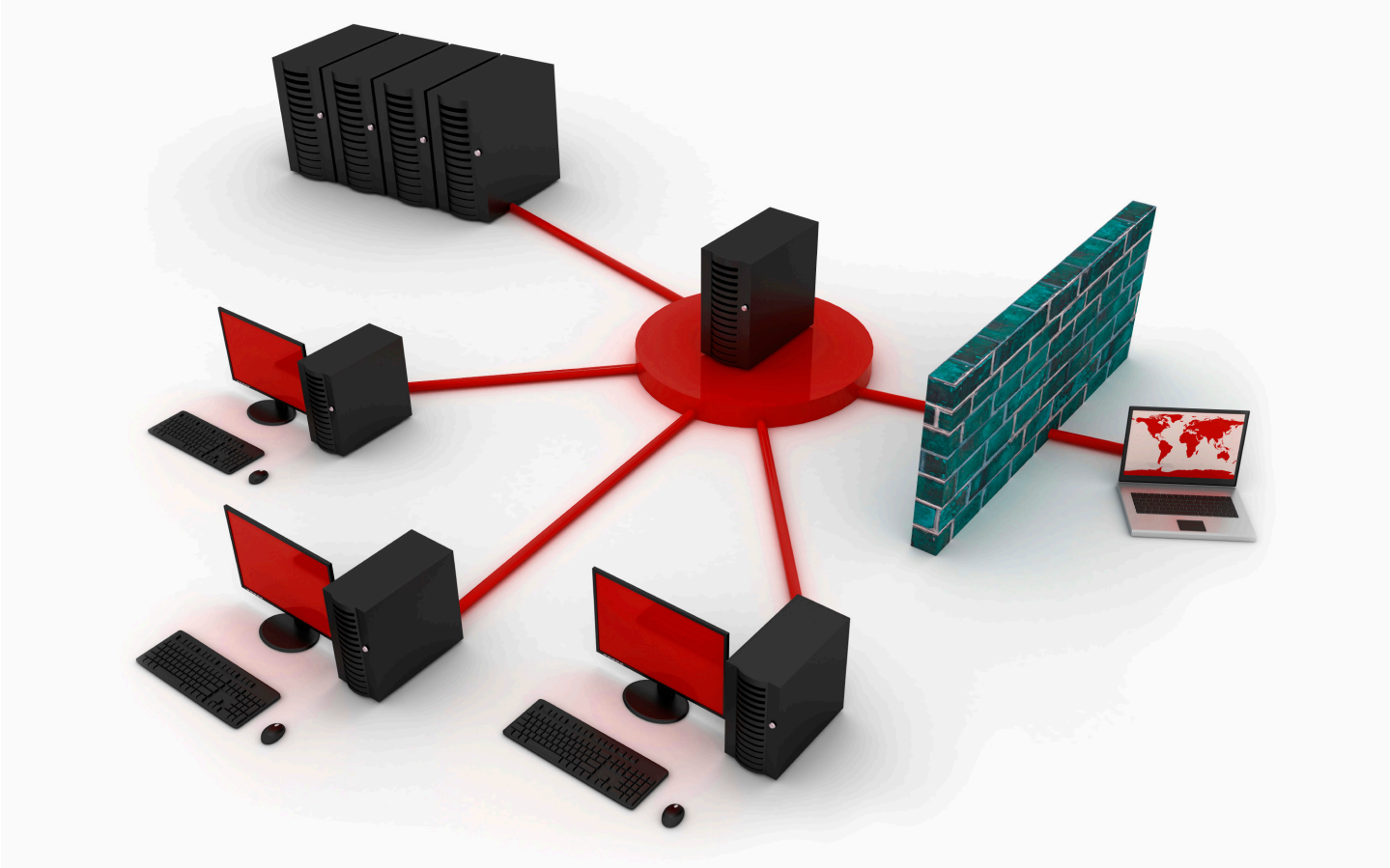
THE IMPORTANCE OF DATA

Data is critical to any organisation, so the key question is: who holds responsibility for data within the organisation?

Data is often pushed down several layers from the board and seen as overly complex and technical. In many organisations, it is the remit of the CIO; in others, the CISO or Chief Data Officer. In financial services organisations, it generally is the responsibility of the Chief Risk Officer as part of the wider financial, operational and prudential risks faced. In many cases, one could argue that the CRO has been elevated to the board of financial services organisations in response to regulatory requirements. As a result, even though most CROs have strong business strategy and risk heritage, many lack technological expertise.

In short, many organisations have no coherent strategy on data and it is often split depending on whether the focus is on money, R&D, customer data or intellectual property. It is critical that issues surrounding data are discussed at board level, particularly the CEO and CIO working with the board to protect company assets and customer loyalty in the same way they protect other areas of the organisation. Data should be jointly evaluated and a decision reached around what is most valuable and what should be prioritised. In addition, when data is promoted to the board, it becomes a commercial driver and there is an opportunity for companies to be seen as a trusted holder of that information and use it intuitively to improve customer experience.

"The new generation of millennials expect companies to know everything relevant about them; they want a tailored buying experience." Heather Jackson, Director, Actinista



CYBERSECURITY AND THE 'CORPORATE BLIND SPOT'

Many board directors are not fully aware of how technological changes are creating new and significant security challenges for their businesses. It doesn't help that many current board directors have spent most of their careers in a pre-internet world.

As a result, the lack of a technology savvy CEO and Chairman is often a 'corporate blind spot' where cyber security is concerned. Amongst CEOs and Chairmen in particular, there can be a feeling of 'tech is below me, I'm more strategy.' Moreover, as a CEO, if you do not know how to leverage technology to effectively strategise against cyber-attacks (and recover quickly following one), then a blind spot clearly exists.

"The challenge lies with the boards that are not technologically literate. Phrases such as: 'I have my secretary print out my emails' and 'I don't know how to use my smartphone properly' and 'Facebook is for my kids' should never be heard."
Al Lakhani, MD, Alvarez & Marsall

Additionally, a CIO who generally sits below the board, or simply that lacks the capability or opportunity to articulate how technology can be monetised is a further imperative to ensure cybersecurity becomes a whole-of-business responsibility.

"If for the last 20 years as a CIO all you've been taught is to invent or deploy the next technology for cutting cost, it can be very difficult to think strategically and communicate in true business terms."
EJ Hilbert, Kroll

Deloitte argues that the CIO should be the lynchpin in the cybersecurity conversation: the visionary, the facilitator, the conduit for information and the challenger of the business. But what happens when the CIO is either not up to the job or does not have the right exposure within the organisation to drive this agenda?

"You would never dream of a CFO not coming to a board meeting. In addition, you would never see a CFO passing up using external audit or teams of external advisors. CFOs also wouldn't be heard saying 'Don't worry; we've got a third party doing that.' The same diligence has to be assigned to cybersecurity."
Val Rahmani, Non-Executive Director, Aberdeen Asset Management

BRINGING CYBERSECURITY TO THE BOARD

Cybersecurity needs to be addressed by a fundamental change in the way a board communicates. CIOs need to move closer to the business and learn to communicate strategically around these issues. CEOs need to move closer to technology and should consider building an advisory board that includes the best strategist and thought-leaders on this issue and, potentially, think seriously about bringing a Non-Executive Director onto the board who has technological expertise. In 2007, Marks & Spencer brought in Martha Lane Fox, co-founder of Lastminute.com and UK Digital Champion, thus showing its commitment to driving its digital agenda. This year, Val Rahmani joined the board of Aberdeen Asset Management following a successful career at IBM specialising in internet security and we predict more companies will follow this lead.

Many companies are unwilling to talk openly about cyber-attacks due to the fear of being stigmatised. This complicates efforts to share best practice and increase cyber awareness at board level. Information between competitors needs to be shared: in the US, the five largest film companies have scheduled monthly round-table meetings to discuss the threats that they are facing in order to pool their intelligence. This approach is slowly being taken up in the UK, but momentum needs to be gained.

CONCLUSION

- Boards must share the responsibility for setting the cybersecurity agenda.
- The CIO should play an important role as the strategic advisor around the technology implications at board level - and the reporting structure should reflect this.
- If there is a dedicated Chief Data Officer then companies should think seriously about where this role reports into.
- If the CIO is not board-ready, non-financial services companies should consider creating a Chief Risk Officer role, developing their existing CIO or hiring a new CIO who is credible to the board.
- Chairmen and CEOs need to educate themselves on the key issues presented by cybersecurity and invest in external expertise or a Non-Executive Director with the appropriate expertise to ensure the right questions are asked.
- Every senior stakeholder needs to be committed to the agenda, as does every person with access to the organisation's facilities, including employees, clients, vendors and third parties.
- Employees as well as boards have to be educated in terms of business technology security and use: personal security behaviour is often overlooked in favour of the macro picture.
- Cybersecurity is not finite and it is not covered by a one-size-fits-all solution; it needs to be treated as an ongoing process with the appropriate measures continually evaluated and the results of these evaluations acted upon.

ACKNOWLEDGEMENTS

British Private Equity & Venture Capital Association (2015) Guide to cyber security
Deloitte (2014) Cyber Security: Empowering the CIO
Ernst & Young (2014) How to use cybersecurity to generate business value
HM Government (2014) Cyber Security: balancing risk and reward with confidence
KPMG (2014) Cybersecurity: it's not just about technology

NORMAN BROADBENT CIO PRACTICE

Adam Turner
Managing Director, CIO & TMT Practice
Adam Turner joined in January 2011 to lead the Private Equity, TMT and CIO Centres of Excellence. His broad experience encompasses many different sectors - private equity, professional services, business process outsourcing, telecommunications, media and across the fin tech/high-tech sector. Functionally, Adam also has in-depth experience in the CIO area, where he has helped both listed and private equity backed businesses.

Prior to joining Norman Broadbent he was the Head of the Private Equity and Technology, Media & Telecommunications and CIO Practices and a Partner in the Board Practice at Odgers Berndston. Adam moved into executive search in 1994 and joined Odgers in June 2004.

Before entering the search industry, Adam worked for Bell Canada and Vodafone. His original search role was with another global search firm, Morgan Howard International, focused in the technology, media and telecommunications sectors. During this time he built operations and search practices globally and his final leaving position was as CEO. Adam has operated with both a national and international remit. He has lived and worked across four continents having successfully completed senior level searches in the UK, USA, Asia and EMEA.

Adam was born in Zambia and has geographic expertise working across the African continent.

Lydia Shepherd
Associate, CIO
Having graduated from Oxford University, Lydia worked as a sales-trader at Citigroup before transitioning into executive search. Lydia then spent three years at a boutique executive search firm delivering senior level technology, telecoms & professional services assignments globally before joining Norman Broadbent in 2012. Lydia is functionally aligned to the CIO practice and has since delivered a number of Fortune 500 and FTSE 350 CIO assignments and a number of other senior level technology and digital roles across a variety of sectors. Alongside executive search, Lydia is involved with Norman Broadbent's Diversity agenda and regularly represents the firm at conferences and government events.

Norman Broadbent
12 St James's Square | London | SW1Y 4LB | Tel: +44 (0) 20 7484 0000 | info@normanbroadbent.com
www.normanbroadbent.com