IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

IT Security

Building Customer Trust – Cybersecurity in CSR Programmes

Jake Olcott

Jake Olcott
Vice President of Government Affairs
BitSight

Biography

Jake Olcott is Vice President of Government Affairs at BitSight (https://www.bitsight.com), where he helps organizations benchmark their cybersecurity programs using quantitative metrics.

He speaks and writes about the role of directors, officers and executives in cyber-risk management. His paper, "The Board's Role in Cybersecurity," was published in 2014 by the Conference Board.

Jake is also a member of the Conference Board's Cyber Governance Advisory Group. He served as Cybersecurity Attorney to the Senate Commerce Committee and House Homeland Security Committee.

He is an Adjunct Professor at Georgetown University, and holds degrees from the University of Texas at Austin and the University of Virginia School of Law.

Keywords Corporate social responsibility (CSR), Cyber risk, General Data Protection Regulation (GDPR), Data breach, Third-party risk management, Cybersecurity, Customer trust
Paper type Research

Abstract

In this article, the author discusses how companies can build customer trust by improving cybersecurity procedures and strengthening communications around cyber risk management, protection and preparedness. In particular, the author explains how cyber risk is becoming increasingly important at board level, as boards begin to realise that the effects of a data breach go far beyond the subsequent financial repercussions, and that this can also have a significant impact on customer trust.

Introduction

In today's evolving cyber risk landscape, Boards of Directors are becoming increasingly concerned[1] about their company's security performance. In fact, the NACD has found that 89% of public companies and 72% of private companies regularly discuss security at Board meetings. That's because directors have become overwhelmingly aware not only that there has been a continual stream of data breaches in the last couple of years, but also that increasing regulation such as the GDPR has raised both compliance risks and public awareness of companies' responsibilities for protecting personal data. Boards are being forced to

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

acknowledge that the effects of a data breach go far beyond the direct hard costs, there is also a significant impact on customer trust.

To put some context around this, the Ponemon Institute Data Breach report[2] published in July 2018 found that the average cost of a data breach has hit an all-time high of $3.86 million, up 10% since 2014. However, according to the report, the hidden or indirect costs of a breach, including notifying customers and any subsequent loss of business, frequently far outweighed the direct costs of fines and legal undertakings. For example, companies that lost less than 1% of existing customers following a breach incurred an average total cost of $2.8 million (£2.1 million), while companies that experienced a churn rate of greater than 4% lost $6 million (£4.5 million) on average.

This considerable potential for financial loss means it's not surprising that cyber-risk, coupled with reputation management, is rising up the board agenda. Directors are striving to understand and quantify cyber risk on the same terms as they assess strategic risk, compliance risk and operational risk.

A further emerging concern for directors is the third-party risk to their business from its supply chain and wider business ecosystem – a compromise of any of those trusted partners could lead to a data breach or systems outage. A recent study by Gartner[3] found that nearly 70% of Chief Audit Executives see third-party risk as one of their top concerns as we head into 2019.

So, how can companies mitigate these risks? Evidence from the Ponemon Institute report shows that organisations which are proactively focusing on building customer trust – both in advance and in the aftermath of a data breach – and raising it to a board level issue are better insulated against the reputational damage caused by breaches. They have reduced the number of lost customers, ultimately reducing the cost of the breach. For example, when a business deployed a senior-level leader, such as a chief privacy officer (CPO) or chief information security officer (CISO), to direct customer trust initiatives, they lost fewer customers and minimised the financial consequences of a breach. Additionally, organisations that offered identity protection to data-breach victims kept more customers than those that did not.

Cyber risk and customer trust – a growing CSR issue

Clearly, improving customer trust and demonstrating transparency are strategically valuable to companies, and it is interesting to see how organisations are tackling this issue and communicating their progress to stakeholders. Of particular note is that cyber risk is no longer the sole preserve of the CIO. The wider potential impact of security failures and data breaches on customer welfare and business sustainability means that it has moved into the realm of corporate social responsibility (CSR).

One of our clients, energy company EDP, is currently the top-rated integrated utility company globally, having achieved the highest Dow Jones Sustainability Index score. They are committed to continuous improvement and transparency in CSR.


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

EDP has identified "improving trust" as a core strategic priority, stating that "trust is an asset that we want to reinforce". The company therefore includes information about the initiatives undertaken and progress achieved towards that target in its annual reports.

When it comes to cybersecurity, EDP recognised that the cyber risk in its extended supply chain should be proactively monitored to protect customers. The company has therefore adopted BitSight Security ratings to continuously assess its own cybersecurity performance and that of its ecosystem of third-party suppliers. This uniform assessment extends sustainability and security principles across the value chain.

By measuring security performance, EDP is driving continuous improvement among its suppliers and quickly identifying any emerging risks. This in turn influences shareholder value by strengthening customer trust and is the reason why the company chose to include its BitSight security rating in its annual CSR report.

Keeping it simple

Key to the success of reporting cybersecurity progress to stakeholders is simplicity. Cybersecurity reports can be complex and opaque – to the extent that even board directors struggle to understand them. An organisation may decide to "improve its security posture" or "change its risk profile" but it can be difficult for wider audiences to understand just what that means.

When reporting at overview level organisations need a simple metric that can be presented as a Key Performance Indicator. This provides a benchmark and can be used to set targets, then demonstrate progress over time. In the case of EDP, their initial BitSight rating on 1 January 2018 was 590, and they set a target to achieve a rating of 640 over the course of the calendar year. The actual rating they achieved by 31 December 2018 was 650, so they were able to clearly and simply demonstrate to a non-technical audience that they had successfully exceeded their target.

Of course, behind that single rating number is a comprehensive analysis into which board directors can delve to glean intelligence on compromised systems and vulnerabilities, security diligence and protocols, user behaviour risks, network infrastructure, and domain infrastructure issues. They can then identify areas for risk mitigation, improvement and investment.

Nevertheless, having that topline benchmark number delivers an at-a-glance indication of how the organisation and its ecosystem is performing. This helps board members quantify security risk more effectively and make informed decisions about issues such as required levels of cyber insurance coverage.

Trust as a business differentiator

In 2019, we will start to see the real impact of regulatory changes such as GDPR and the public profile of organisations that have suffered breaches will be seriously tested. I believe that we will see more companies become proactive about

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on our main website at **www.creditcontrol.co.uk**.

improving customer trust and transparency around cybersecurity and data protection, aiming to minimise the "soft" costs of breaches that, in today's security environment, are inevitable.

As the way that cybersecurity is viewed by organisations and end users continues to mature and develop, we will see more and more companies strengthen their communications around cyber risk management, protection and preparedness, presenting trust as a business differentiator. They will make this part of their CSR programme as well as their security programme in a bid to mitigate risk not just on a financial level, too.

Reference

1 https://www.wsj.com/articles/boards-seek-bigger-role-in-thwarting-hackers-1515596400

2 TWO - https://www.ibm.com/security/data-breach?ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&cm_mc_uid=05318305163115235184421&cm_mc_sid_50200000=36495741532685877922

3 https://www.gartner.com/en/newsroom/press-releases/2018-10-25-gartner-says-data-and-analytics-risks-are-audit-executives-prime-concerns-for-2019