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 **https://www.itceoscfos.com**

Cybersecurity

The CrowdStrike Outage – Painful Losses, Operation Challenges and Reputational Risk

Nick Hood

Nick Hood
Senior Business Advisor
Opus Business Advisory Group

Biography

Nick Hood is the Senior Business Adviser at the Opus Business Advisory Group (https://www.opusllp.com), the largest independent advisory, restructuring and insolvency firm in the UK.

Nick was a licensed Insolvency Practitioner, working in the business rescue market for 25 years. He is a committed internationalist, having created the largest global network of independent business rescue firms and having also worked overseas in Canada, Milan and Bahrain.

In his earlier career and after qualifying as a Chartered Accountant in 1970, Nick held senior executive positions in major companies in the construction, engineering and media sectors, as well as working for a boutique investment bank.

Nick's thought leadership and opinion blogs for Opus can be found at https://opusllp.com/resources/.

Keywords Cybersecurity, Cyber-attack, IT, Software, Resilience, Disaster recovery, Reputation, Technology, Risk, Backup plan
Paper type Opinion

Abstract

The CrowdStrike outage has caused huge public service and commercial disruption worldwide as 8.5 million devices started displaying the IT world's ultimate nightmare – the 'blue screen of death'. The financial effect will unfold over time as affected companies publish their accounts, but the operational challenges were immediate. Repairing the damage to their reputations will take time and require top class communication skills as the author of this article explains.

Introduction

Parametrix, the IT outage risk consultants estimates that the recent global IT disruption linked to CrowdStrike that impacted some 8.5 million Windows-powered devices could cost Fortune 500 companies (excluding Microsoft) at least $5.4 billion in direct financial losses[1].

Perhaps no more than 20% of this huge sum and the additional losses suffered by other smaller companies and institutions may be covered by insurance because of large risk retentions, policy limits and policy wording.

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 **https://www.itceoscfos.com**

The net losses after insurance recoveries are a serious financial issue for each and every business effected, most of all for smaller entities without the same level of resources and sophistication as their larger brethren. The potential financial impact of this sort of situation can be seen from the iconic retailer, Carpetright, where the loss of a week's trading[2] because of a cyber-attack earlier this year has been singled out as a major factor in its collapse into Administration.

As well as pure financial effects, there will be an impact on how businesses are run from an operational standpoint and there are very real risks of reputational damage from letting down customers and clients.

Cyber security context

The CrowdStrike outage was not the result of a cyber-attack, but instead was the result of a faulty software update of the widely used Falcon sensor security software. Nevertheless, its impact highlights the high level of reliance on technology built into the operational models of businesses.

The downside of this situation is the increasing frequency of cybersecurity issues. Research by cyber consultants, SoSafe revealed that half of security professionals have experienced a successful cyber-attack in the past year and 55% in the UK reported that their company had been negatively impacted. Some 85% of UK


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 **https://www.itceoscfos.com**

respondents confirmed that the threat levels were now the highest and most challenging in the past five years.

Cyber Security & Resilience Bill (CSRB)

The significance of the bandit territory that cyberspace has become and the potential effects on the corporate world has prompted the new government to step in with legislation to impose some responsibilities on businesses and other public bodies. This new law aims to make sure that they can survive and recover from cyber-attacks and software failures.

Its two main features are a requirement for mandatory and timely reporting of cyber incidents to facilitate “collaboration between businesses and government agencies to mitigate the impact of cybersecurity breaches” and to require businesses to “develop and maintain comprehensive resilience and recovery plans”.

Management responsibility

Businesses shouldn’t need a CrowdStrike moment or government legislation to prompt them to protect themselves from cybersecurity risk that can cause devastation and destruction. Arguably, their fiduciary responsibility to stakeholders such as shareholders and in some circumstances, creditors mean they are obliged to get ahead of this potential downside. The problem is that senior management often don’t understand this particular risk in sufficient detail.

Significantly, the CSRB emphasizes “enhanced accountability”, requiring senior management and board members to be actively involved in overseeing cybersecurity measures and ensuring their company’s compliance with the legislation.

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 **https://www.itceoscfos.com**

Operational impacts

Much of these are simple and obvious, but equally dealing with some of them is a challenge far too easily hidden away in someone's 'too hard' file:

- **Have a back-up plan** – There needs to be both a business continuity and a disaster recovery plan in place. Otherwise, the survival of the whole business is at risk. If a cloud provider goes down, a ransomware attack happens, or data is suddenly corrupted, hacked or deleted, there must be recoverable data backups, as well as an analog plan of action.

  The CrowdStrike outage came from a technical software defect, but it was the lack of a workable Plan B at so many of the businesses affected that really caught the public and media attention. Whether the business is a cash-free cafe, a multinational airline or a hospital, employees need to have been trained on how to deal with a sudden shift back to analog. At the very least, key records should be available as a backup in a non-digital format and kept securely, so operations can continue when systems go down.

- **How robust are your service providers?** – A business might have effective cybersecurity of its own, but how much attention does it pay to similar arrangements at key service providers? The cybersecurity of third-party service partners should be reviewed regularly, and steps taken to ensure there is a backup plan for each provider going down. Single points of failure should be avoided, if possible, but at the very least they should be identified.


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 **https://www.itceoscfos.com**

As Microsoft put it in its post-CrowdStrike announcement: "this incident demonstrates the interconnected nature of our broad ecosystem – global cloud providers, software platforms, security vendors and other software vendors, and customers".

- **Involve employees as stakeholders in cybersecurity** – A key strategy for flagging up potential cybersecurity issues is treating employees as stakeholders and developing a 'no blame' culture, so that potential problems can be identified, shared and rectified before something to goes wrong, rather than after a cyber disaster. Staff may have a far more informed view of unjustified risks being taken in this area than any management board, which may be kept in the dark by a self-protecting IT department.

  CrowdStrike itself may turn out to be the prime case study on this aspect if it turns out that speed of delivery of the particular software change was prioritized over pre-testing, quality, reliability and security. In a different industry, there is an obvious parallel with the safety standards debacle at Boeing, where staff concerns were suppressed rather than listened to.

- **Remember the human vulnerability issue** – The SoSafe research highlighted human vulnerability as the single most common origin for successful inbound cyber-attacks. The commercial world has become ever more dominated by automation, where systems are checked by other systems, sometimes with complete disregard to human behavioural factors. Businesses should be taking a more holistic, behavioural approach to reinforcing their cyber defences.

- **Don't scrimp on the cybersecurity budget** – Organizations habitually underinvest in IT, blindly trusting third-party vendors as the magic way to stay safe. This is why updates can be done automatically and routinely without anyone at the software end-user testing them out first. The CrowdStrike incident is a painful reminder that software can be broken not just by the user's own code, but by its dependencies and third-party vendors.

There are powerful arguments that endpoint protection software is inherently dangerous because it must be given privileged access to the operating system to be effective. The CrowdStrike driver (which they call a "sensor") is so deeply buried inside Windows and bypassed by routine Windows safeguards, that the update error was able to take out entire operating systems.

The only defence against all this external influence on a company's vital operations is to allocate sufficient financial and internal skilled human resources to be able to challenge this imbalance of power and fend off the threats when external providers' agendas threaten the resilience of the user. The IT (and cybersecurity) function must also have an effective voice in setting the strategy of the business It serves.

Reputational issues

The outage may have been the fault of CrowdStrike, but the reputational damage (at least outside the world of cybersecurity) fell on the software end users as a

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 **https://www.itceoscfos.com**

range of services to the public (airports, hospitals, etc) fell apart temporarily and a huge number of businesses ground to a halt, which will have let down incalculable numbers of customers and clients. Ironically, there has been almost no immediate public criticism of Microsoft.

Beyond restoring services to normal as quickly as possible and compensating customers where appropriate without hiding behind nitpicking interpretations of the fine print of customer contracts, it will be important now for the affected businesses to communicate openly and constructively with customers about what happened and what steps they are taking to minimize (so far as possible) the chances of anything similar happening in the future and mitigating the impact if it does.

Doing nothing to reassure customers is not an option. They have long memories and even for those that don't, the media will be quick to remind the public about the CrowdStrike outage the moment any sort of repeat incident occurs.

Reference

1 Robins-Early, N. (24 July 2024), 'CrowdStrike global outage to cost US Fortune 500 companies £5.4bn'. The Guardian. Available at: https://www.theguardian.com/technology/article/2024/jul/24/crowdstrike-outage-companies-cost

2 Morgan, A (23 April 2024), 'Carpetright unable to trade after cyber attack'. Retail Gazette. Available at: https://www.retailgazette.co.uk/blog/2024/04/carpetright-cyber-attack/