CYBER INSIDERS: A BOARD ISSUE

Cyber security is an issue on the agenda for most boards. The insider threat generally receives less attention. As a result, the human factors aspects of cyber security can become the weak link in organisations' cyber defences, leaving the organisations vulnerable and their boards open to criticism and reputational damage. This article explores the subject of cyber insiders and the key measures all boards should take to ensure that their organisation is appropriately protected against this threat.

By Chris Hurran, OBE. Senior Associate Fellow of the Institute for Security and Resilience Studies at University College London.

Institute for Security & Resilience Studies

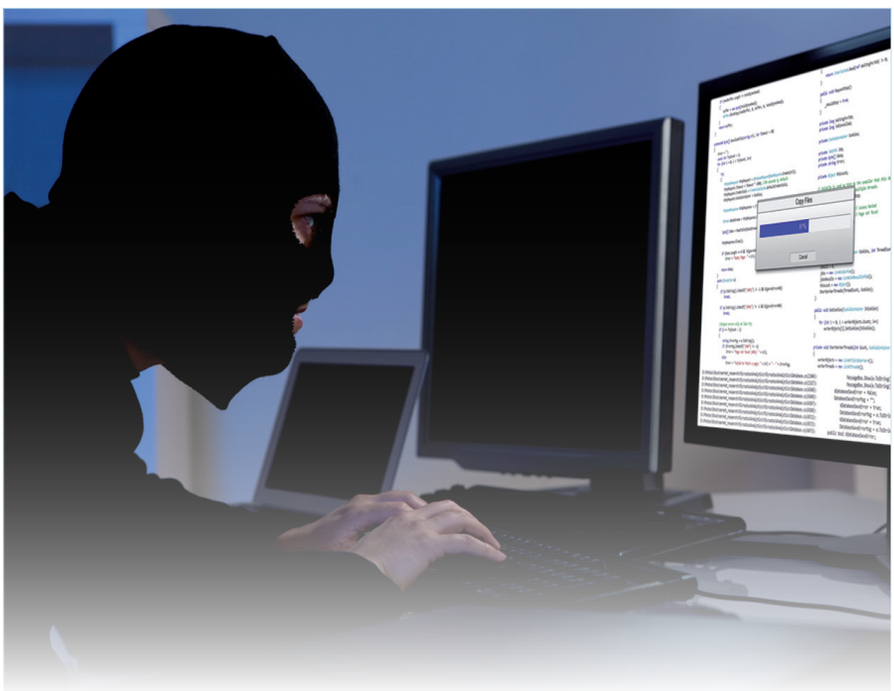
INTRODUCTION

Boards are increasingly concerned about the threat to their business from cyber-attack. Businesses invest significantly in technical measures to protect their assets and they employ highly qualified and highly paid technical experts to deliver this protection. Alternatively, they may attempt to outsource the whole problem by paying others to provide the protection on their behalf. Of course, technology and high priced help have an important role to play in cyber security, but all this investment can be undermined all too easily from another source – **the organisation's own employees**. There is limited definitive data on the scale of this issue, but the PwC 2013 Information Security Breaches Survey[1] indicates that 36 per cent of the worst security breaches in the year were caused by inadvertent human error (and a further 10% by deliberate misuse of systems by staff), and 57% of small businesses suffered staff-related security breaches in the last year. So this is a non-trivial problem and boards ignore it at their peril.

THE EMPLOYEE AS A CYBER INSIDER

Who are these troublesome employees? Cyber insiders can come from any part of the business (including the board itself!) and manifest themselves in three types:

Non-malicious and unintentional: These employees do not mean to do anything wrong. The fact that they cause harm is the organisation's fault. Either unsuitable people were recruited; or they were not trained properly; or the security culture is defective; or the organisation



does not have an appropriate and continuing cyber security awareness programme; or the managerial oversight isn't doing its job. Don't blame the people.

Non-malicious and intentional: These employees are harder to deal with because they can include the most loyal, committed and hardworking employees. But the business process and culture in the organisation fails to dovetail with the management of cyber risk. These are the people who e-mail work home so they can do it over the weekend or share passwords because they cannot deliver their work any other way. These employees are forced to make their own risk judgements because the organisation has not taken responsibility for doing it. Sometimes these employees' judgements turn out to be flawed. Once again, don't blame the people.

Malicious and intentional: These employees can cause the most serious harm, especially with the enormous power of cyber technology at their disposal, but fortunately they are also the rarest. A significant research contribution on this phenomenon can be found in the Insider Study carried out by the Centre for the Protection of National Infrastructure[2]. This study is about insiders generally, not exclusively cyber insiders, and it focuses only on malicious acts. It is an ongoing piece of research which started in 2007 and which will continue into the future. It is not a quantitative study – "what is the scale of the threat" – but a qualitative one. The CPNI experts have investigated in depth some 120 cases of significant insider harm taking place across the public and private sectors. They have focussed on the characteristics of the people that committed the harmful acts and also, importantly, **the characteristics of the organisations that enabled the acts to take place**. The report highlights the clear link between an insider act taking place and exploitable weaknesses in an employer's protective security and management processes. Nine organisational-level factors are identified in the report but they include:

- Poor communication between business areas and,
- Lack of awareness of people risk at a senior level and inadequate corporate governance.

In the case of these employees who maliciously and intentionally carry out harmful acts we **must** blame the people. But we also need to place some of the responsibility for the insider event on the organisational enabling factors. If these had been addressed the possibility of the event taking place would have been reduced.

It is clear that cyber insiders of all three varieties can be employees working in any part of the business and that therefore addressing this complex problem is an issue for the business as a whole. It needs to be addressed in a way that does not negatively impact on business delivery, it is not a risk that can be outsourced to others and it cannot be solved solely by technical solutions (even if technology may make a vital contribution to mitigating cyber insider risk). Business-wide issues need leadership from the board.

... WE ALSO NEED TO PLACE SOME OF THE RESPONSIBILITY FOR THE INSIDER EVENT ON THE ORGANISATIONAL ENABLING FACTORS …

THE BOARD RESPONSE

Every organisation will have to tailor its response to the cyber insider threat in a way that meets its own particular business needs. But there are common themes for all organisations irrespective of size, sector or business model. These common themes could be described as "10 Steps to Cyber Insider Protection" and are:

1. **Governance:** recognising that ownership and accountability for different aspects of people risk should not be divided at board level, there is a single board level owner of all aspects of people risk in the organisation.
2. **Roles, responsibilities and resources:** having identified a single point of ownership for people risk on the board, roles and responsibilities for managing different aspects of people risk from the top down are clearly understood by all and the measures and procedures involved are appropriately integrated and resourced.
3. **Assets:** the board fully understands the organisation's critical assets and their vulnerabilities. Recognising that the criticality of assets varies with circumstances (e.g. data relating to mergers and acquisitions activities) there is a review process in place to constantly update the list of critical assets.
4. **Risk:** the organisation conducts a full formal review of insider risk at least annually; insider risk is on the top risk register and the board is fully sighted on the specific groups of employees who constitute the highest level of risk and on the mitigating measures in place to manage that risk; the board has proactively articulated its attitude to insider risk tolerance and this is understood in the organisation and feeds into security culture.
5. **Culture:** the board has agreed the desired security culture for the organisation and an appropriate plan is in place to move towards achieving it. Once achieved it will be routinely monitored for performance and success criteria and the delivery of operational benefits.
6. **Impact:** the board understands the impact (including operational, financial, reputational and legal) that an insider incident would have on both the organisation and on the board itself.
7. **Response:** the organisation is appropriately prepared to react in response to an insider event, to minimise harm and to maximise possibility of attribution and appropriate action with respect to the perpetrator. Response is practised through an exercise program (including at board level).
8. **Transparency and awareness:** all measures and procedures (including employee monitoring if used), whistleblowing, employee performance assessment, etc.) are enshrined in policies which are proportionate, compliant with legal and regulatory frameworks (e.g. the ICO's Employment Practices Data Protection Code [3]) and are fully visible to and understood by employees. Employees are aware of the potential consequences of engaging in an insider act.
9. **Supply chain:** recognising that risk cannot be outsourced, the board level owner of people risk ensures that all aspects of people risk mitigation and asset management include the supply chain. Procedures and policies applicable to employees (including pre-employment screening, aftercare, etc.) are equally applicable in the supply chain (especially outsourced security functions), are enshrined in contracts and are audited and performance managed.
10. **Audit:** the audit committee reviews the overall management of insider threat on an annual basis with particular emphasis on ensuring that risks and assets are regularly reviewed and are current and that the policies and procedures involved are functioning well, properly integrated, and compliant with legal and regulatory frameworks.

... EMPLOYEES ARE AWARE OF THE POTENTIAL CONSEQUENCES OF ENGAGING IN AN INSIDER ACT ...

... DAMAGING INSIDER ACTS CAN CAUSE CATASTROPHIC HARM TO THE ORGANISATION'S OPERATIONS, ASSETS AND REPUTATION AND LEAVE THE BOARD ITSELF OPEN TO LEGAL, REGULATORY AND/OR OVERSIGHT CONSEQUENCES …

CONCLUSION

High performing organisations typically have an effective and visible people risk reduction programme, with a single point of ownership and accountability on the board, and a holistic approach to all people, process and technology aspects of insider risk management across the organisation. This visible top management leadership of the programme underpins an appropriate, organisation-wide security culture and deters most insider acts. Understanding that damaging insider acts can never be entirely excluded, the board has a response plan to minimise harm, protect the operations, assets and reputation of the organisation, and to detect, identify and prosecute insiders.

Conversely, organisations in which the board pays lip service to insider risk, security functions are considered to be esoteric subjects left to middle ranking security professionals, those functions are stove piped in silos which lack mutual visibility, and the board has little understanding of the organisation's critical assets and their vulnerability, are very vulnerable to damaging insider acts. Such acts can cause catastrophic harm to the organisation's operations, assets and reputation and leave the board itself open to legal, regulatory and/or oversight consequences. ■

REFERENCES

1 *PwC (2013) 2013 INFORMATION SECURITY BREACHES SURVEY*, Available at: http://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf (Accessed 30 April 2014)

2 *CPNI (2013) CPNI INSIDER DATA COLLECTION STUDY: REPORT OF MAIN FINDINGS*, Available at: http://www.cpni.gov.uk/documents/publications/2013/2013003-insider_data_collection_study.pdf?epslanguage=en-gb (Accessed: 30 April 2014).

3 *ICO (2011) DATA PROTECTION: THE EMPLOYMENT PRACTICES CODE* http://ico.org.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/the_employment_practices_code.pdf (Accessed: 30 April 2014).

ABOUT THE AUTHOR

Chris Hurran, OBE, is Senior Associate Fellow of the Institute for Security and Resilience Studies at UCL, a Director of Cyber Security Challenge, and Vice President (Acquisition) of the Trustworthy Software Initiative. As an independent consultant, Chris advises organisations how to mitigate the risk of harm caused by their own employees.