CYBER INSIDER RISK MITIGATION MATURITY MATRIX

By Chris Hurran, OBE, Senior Associate Fellow of the Institute for Security and Resilience Studies, UCL

Cyber security is increasingly recognised to be a people issue as much as a technical one. Boards now understand that their own employees may be the weak link in an organisation's cyber defences. This article provides a self-assessment matrix to help organisations understand how effectively they are mitigating cyber insider risk and thus enable them to embark on a programme of improvement.

INTRODUCTION

Cyber Insiders – a Board Issue (Cyber Security Review, Summer 2014 edition[1]) attracted considerable interest. For many readers the distinctions between cyber insiders who could be "witting or unwitting" and "malicious or non-malicious" were novel. Many had previously been unsighted on CPNI's excellent insider threat research[2] and the evidence that indicated the existence of nine factors at organisational level that enable insider acts to take place. Most readers accepted that the proposed "10 Steps to Cyber Insider Protection" were a valuable approach to addressing the organisational level factors which enable insider acts to take place.

In the two years since ***Cyber Insiders – a Board Issue*** was published there have been some developments. For example:

- There have been eye catching examples of the scale of harm that cyber insiders can cause.
- The improvements in network defences have led to malicious actors using increasingly sophisticated and targeted attempts to turn an organisation's employees into unwitting insiders (e.g. through social engineering, spear phishing etc).
- Boards have increasingly been held to account for the consequences of cyber-attacks, including those caused by insiders. This accountability will increase in the near future through regulation (including, for example, GDPR).

In short, the need for Boards to address cyber insider risk (CIR) is now well understood. What is less well understood is what to do about it. There is still a tendency to seek to outsource CIR or to regard it as chiefly as a technical problem with a need for some additional staff awareness training. This approach is likely to leave organisations vulnerable to CIR.

CYBER INSIDER RISK MATURITY (CIRM) MATRIX

Although readers of ***Cyber Insiders – a Board Issue*** saw the value of the proposed "10 Steps to Cyber Insider Protection" approach, some frustration was expressed that more was not said about how to address these issues. Above all there was a sense that it was not possible to assess what "good" looked like in the context of CIRM. This CIRM Matrix is an attempt to close that gap. It is not intended to be a quantitative assessment tool and there is scope for it to be used in a variety of ways. For example a CISO could use it as a checklist of areas to cover, while researching for detailed evidence in order to assess CIRM against each of the 10 attributes. Alternatively a board could use it to support a more subjective Board discussion of CIRM. However it is used, it is likely to provide pointers to the areas which need addressing in order to enhance an organisation's CIRM.

	Low: Initial measures and awareness	Medium Low: Developing measures	Medium: Competent, business enabling measures
Governance	Board commitment to CIRM, if it exists, is neither demonstrated nor visible. No Board awareness of CIRM processes or policies.	Board commitment to CIRM is neither demonstrated nor visible. Board members aware of CIRM processes or policies in their own business silos. Collective Board engagement in CIRM only in response to incidents.	A single Board level owner of all aspects of people risk in the organisation including CIRM. Visible Board commitment to CIRM and Board awareness of CIRM processes and policies.
Roles, responsi-bilities and resources	No corporate CIRM policy or programme. Any CIRM activities carried out are in uncoordinated business silos and resourcing is secondary to other business priorities.	Senior members of staff have responsibility for discreet areas of CIRM. CIRM policy exists but is not shared beyond those working in the security function. Overall, CIRM is inadequately resourced.	A corporate CIRM policy which is available to the whole business. A single CIRM programme with responsible senior managers coordinating their activities and reporting collectively to the Board level owner of the CIRM programme. CIRM adequately resourced.
Assets (see Note 1)	Critical assets which may be at risk from insider events may not have been identified.	Some corporate understanding of tangible, intangible and information assets but this may not be complete and/or up to date. Criticality may not have been established.	The organisation has a comprehensive understanding of its tangible, intangible and information assets which was up to date at the time of the last CIR assessment and which includes clarity on criticality.
Risk	No process for conducting a organisation-wide CIR assessment. CIR is not on corporate risk register.	There is an organisation-wide CIR assessment but it has been carried out on the business by those with security functions and without business engagement. CIR not on corporate risk register. CIRM almost exclusively a focus area for specialists and the responsibility of only a few personnel.	An organisation-wide CIR assessment, conducted with the full engagement of the business, has assessed the risk to critical assets from a full range of insider events including cyber insiders. High risk roles across the organisation have been identified accross the organisation. The most critical CIRs are elevated to the Board on the corporate risk register.
Culture	Board has not considered the organisation's security culture. Staff concern for organisational security does not feature in the workplace.	Board has not considered corporate security culture and senior leadership are inconsistent in their approach to developing an effective security culture. Principles for CIRM may be documented but are not incorporated into business processes. Accountabilities relating to CIRM are not clear or communicated. No promotion or culture of reporting security breaches, and no support for staff in implementing good CIRM practices.	Board has clear understanding of existing corporate security culture and clarity about the desired security culture as part of CIRM. There is a culture change programme in place to achieve the latter. Values and aspirations for CIRM are clearly communicated and are consistently understood throughout the organisation. Staff are encouraged to report security breaches and are comfortable doing so. Security is understood to be the responsibility of all members of staff and this is supported by appropriate awareness training on induction and regularly thereafter.

Medium High: Effective, quantitatively managed programme	High: Excellent and fully optimised programme
A single Board-level owner of all aspects of people risk in the organisation including CIRM. Visible Board commitment to CIRM and the Board proactively engages with the CIRM programme including monitoring KPIs.	A single Board-level owner of all aspects of people risk including CIRM. Visible Board commitment to CIRM. Full Board awareness of CIRM processes and policies. CIRM embedded as an essential element of the proactive and holistic corporate approach to security and operational capability.
Corporate CIRM policy proactively communicated to the whole business. A single CIRM programme with responsible senior managers coordinating their activities and reporting collectively to the Board level owner of the CIRM programme. Managers at all levels fully engaged and understand their role in delivering the CIRM programme. CIRM fully resourced and managed in order to deliver value for money.	Corporate CIRM policy fully integrated with other business activities, proactively communicated to the whole business and regularly reviewed. CIRM programme fully coordinated across the business. Programme governance assures compliance across the business and effective delivery of KPIs. Managers at all levels fully engaged and understand their role in delivering the CIRM programme. CIRM programme fully resourced and managed to deliver value for money and reduced CIR.
The organisation has a comprehensive understanding of its tangible, intangible and information assets and keeps this understanding under regular review in order to proactively intiate CIR assessment for critical assets when necessary.	Board has comprehensive understanding of its tangible, intangible and information assets and keeps this understanding under regular review. Impact of cyber insider events on critical assets is costed and informs both the Board's appetite for risk tolerance and value for money delivered by the CIRM programme.
An organisation-wide CIR assessment, conducted with the full engagement of the business, has assessed the risk to critical assets from a full range of insider events including cyber insiders. The most critical CIRs are elevated to the Board on the corporate risk register. Indicators of security performance are monitored and evidence is presented to the Board to inform strategic CIRM decision making.	CIRM firmly embedded in strategic risk management including explicit clarity of the Board's attitude to CIR tolerance. Corporate CIR assessment formally reviewed at least once every 12 months and additionally when significant changes occur within the business that may impact the risk assessment. CIR considered to be a normal business risk and routinely taken into account by managers at all levels as part of normal business activity.
Board actively monitors the culture change programme in place to achieve the desired security culture as part of CIRM. Board and managers at all levels visibly demonstrate commitment to the desired security culture. Values and aspirations for CIRM are clearly communicated and are consistently understood throughout the organisation. Security is understood to be the responsibility of all members of staff and this is supported by appropriate awareness training on induction and regularly thereafter. Staff know what good security behaviours look like and challenge and/or report bad ones when they see them.	All personnel actively identify with and take responsibility for CIRM policies and practices. Compliance with security policies and procedures (including CIRM) is managed through positive incentives as well as through enforcement practices. CIRM is treated as a core competency. Transparency and accountability are the norm. Leaders work collectively and visibly to encourage innovative ways to continuously improve CIRM. All staff are comfortable identifying risks and opportunities for improvement and new insights are acted upon collaboratively. The Board leads these behaviours through their own example and engagement.

Impact	Board has never considered the potential impact that a cyber insider act could have on the organisation. Employees do not perceive cyber insider acts as having any consequences for them.	Board may be aware of the impact that a cyber insider incident might have on both the organisation and on the Board itself but this is not sufficient for them to give any prioity to CIRM. Employees may have been warned of the possible consequences to them of engaging in a cyber insider act but are aware that previous incidents have usually been ignored.	Board is aware of the impact (including operational, financial, reputational and legal) of a cyber insider incident and therefore takes CIRM seriously. Employees are aware of the potential consequences to the organisation of them of being involved in non-malicious and unwitting cyber insider acts and understand the importance of self-reporting. Employee awareness of consequences deters them from engaging in malicious cyber insider acts.
Response	Corporate business continuity plan (if it exists) concentrates exclusively on conse-quence management and has no focus on cyber insider incidents. No procedure for investigating workplace behaviour of concern or people related security incidents.	Corporate business continuity plan focuses exclusively on consequence management and has no focus on cyber insider incidents. Cyber insider incident response processes are informal, managed within teams and have limited central oversight. No procedure for investigating workplace behaviour of concern or people-related cyber security incidents.	Corporate crisis planning includes specific arrangements for responding to actual or potential cyber insider incidents. Incident recording, response and escalation processes and responsibilities are well documented and followed. Senior managemers receive reports on security incidents, measures taken to remedy them, and any disciplinary action taken. Reporting on the most serious incidents escalated to Board level.
Transparency and awareness (see Note 2)	No reliable pre-employment screening processes in place. HR carry out minimum checks to ensure compliance with employment legislation and HR staff given no relevant training to carry out their duties (eg document verification). No ongoing personnel security measures in place. No ongoing monitoring or assessment of employees by technical or other means.	HR checks by appropriately trained staff ensure compliance with employment legislation. Generic pre-employment screening policy and process for all employees. If pre-employment screen-ing outsourced, no attempt is made to audit the third-party screening provider for compliance. If pre-employment screening is carried out in-house, screening staff may lack adequate training and experience. Employees may take up employment in advance of pre-employment screening checks. Poor levels of line manager training and awareness of CIRM procedures. Reporting and other assurance activities are informal and occur only as issues (e.g. breaches) arise. No holistic monitoring or assessment of staff security awareness or security be-haviours is in place. IT monitoring and/ or audit (where it occurs) takes place within the IT security silo and insider events (eg IT policy breaches) are treat-ed as IT events. Staff job objectives do not include reference to protective security. Assurance activity is ad hoc.	Corporate pre-employment screening policy meets all employment legislation requirements. Security screening proportionate, risk-assessed and role-based. Trained staff conduct in-house pre-employment screening checks. Outsourced pre-employment screening standards contractually specified and subject to audit. Screening not repeated on change of role. Some employees may take up employment in advance of pre-employment screening checks. Security training embedded within business as usual including appropriate training during induction, on changing roles, on major changes to security policies, and on an annual basis. Effective exit procedures in place that include the revocation of electronic access and the retrieval of assets. Holistic monitoring and assessment of staff security awareness or security behaviours by technical and other means. Reporting lines and responsibilities are clear and there is regular management reporting.
Supply chain	The organisation gives no consideration to CIR in its supply chain.	Managers responsible for discrete aspects of CIRM have extended this to parts of the organisation's supply chain for which they are responsible. This is achieved by standard wording in contracts and is not subjected to audit.	CIRM programme extends into the organisation's upstream and downstream supply chains in a coordinated manner which prioritises protection of the most critical assets. Standard contract wording and/or mandating compliance with agreed standards is used. Audit carried out ad hoc or reactively in response to incidents.
Audit	CIRM is not audited.	CIRM measures only audited reactively in response to incidents.	CIRM programme may be audited (including reactively in response to incidents) but not as part of the regular audit schedule.

Board is fully aware of the impact that a cyber insider incident would have. This awareness drives its attention to CIRM KPI reporting. Employee awareness of the potential consequences to the organisation of non-malicious and unwitting cyber insider acts promotes self-reporting and discussion within teams of possible concerns. Employee awareness of consequences deters them from engaging in a malicious cyber insider acts.	The Board's clear understanding of the potential impact of the full range cyber insider incidents informs its critical decision making on CIRM and risk tolerance. Employees are deterred from engaging in malicious cyber insider incidents because of the high probability of being identified and the certainty of serious employment consequences.
Comprehensive, holistic and consistent corporate approach to cyber insider incident management, and well defined hierarchy of escalation triggers. This response plan is well understood across the organisation and is exercised regularly. Security incidents are well reported and root cause analysis is performed to inform process improvements. There is a process in place for recording and reporting on incidents, trends, risks etc.	Ongoing research into measures for preventing and managing cyber insider incidents proactively informs business processes and systems. This research draws on both detailed "lessons learned" from the organisation's own cyber insider incidents as well as awareness of cyber insider events in other organisations. All cyber insider incidents are managed in accordance with the organisation's established response plans.
Corporate pre-employment screening meets all employment legislation requirements. Security screening proportionate, risk-assessed and role-based. Trained staff conduct in-house pre-employment screening checks. Outsourced pre-employment screening standards contractually specified and audited. Screening repeated on change of role on a risk-assessed basis. Employees never employed in advance of full pre-employment screening. Ongoing security training embedded within business as usual. Access to assets controlled according to job role. Exit procedures include revocation of electronic access, retrieval of assets and exit interviews. Holistic monitoring and assessment of staff security awareness or security behaviours by technical and other means. Reporting lines and responsibilities are clear and there is regular management reporting. All staff enabled to report security concerns. Monitoring, assessment and reporting outputs feed into enhanced CIRM.	Comprehensive, corporate pre-employment screening policy and procedures effectively delivered by appropriately trained staff (in-house or third-party screening provider). Security check integration with recruitment process prevents prospective employees receiving unconditional job offer which they are unable to take up on security grounds. Proposals for reallocation of responsibilities include assessment of security clearance requirements. Screening repeated on change of role. Staff commitment to corporate security policies and values, including regular training and development. Access to assets controlled according to job role. Comprehensive exit procedures include enhanced monitoring in last 30 days. Appraisal process includes assessment against a security objective. Holistic monitoring and assessment of staff security awareness or security behaviours by technical and other means. Reporting lines and responsibilities are clear and there is regular management reporting. Staff enabled to report security concerns. Monitoring, assessment and reporting outputs inform enhanced CIRM.
CIRM programme extends comprehensively into upstream and downstream supply chains. Bespoke contractual arrangements ensure CIRM of critical assets. Compliance by suppliers is assured through regular audit.	CIRM programme extends into upstream and downstream supply chains. CIRM measures championed in supplier community. Bespoke contractual arrangements ensure CIRM of critical assets. Evidence of suppliers' CIRM programmes form part of the competitive procurement process. Compliance by suppliers assured by regular audit.
CIRM programme is subjected to regular audit, reporting back to the Board.	CIRM programme regularly audited (at least annually). Emphasis on ensuring that risks and assets are regularly reviewed and are current and that the policies and procedures involved are functioning well and are compliant with legal and regulatory frameworks.

NOTES

1. **Assets:** Tangible assets include people, premises and locations, plant and equipment (including IT hardware), money and e-currency, and materials. Intangible assets include reputation, business volume and staff and public well-being. Information assets include intellectual property or intelligence, commercially sensitive business information, personal data, procedures, processes and software, and access data. In the case of information assets it is critically important to have a detailed understanding of where they are stored and processed (e.g. on servers, on devices and in the cloud).
2. **Transparency and awareness:** All CIRM measures and procedures should be enshrined in policies which are proportionate, compliant with legal and regulatory frameworks and are fully visible to and understood by employees. This row of the maturity matrix covers mainly pre-employment screening, ongoing personnel security measures and employee monitoring. Exemplar details only are provided in this row. For more detailed information, the CPNI good practice guidance on these subjects is recommended (see references). Neither the CPNI guidance nor this CIRM matrix specify particular technical monitoring tools or approaches (e.g. data loss prevention, end point monitoring, behavioural analytics, psycho-linguistic analysis of email message content etc). It is for the organisation to decide which tools and approach best suit its needs. However the key point is that whatever tools are used they should add value to corporate CIRM and the outputs must be firmly integrated to the holistic approach rather than being operated in an isolated IT security silo.

INTERPRETATION

Use of the maturity matrix should indicate an organisation's overall ability to mitigate CIR. If the responses to the various attributes are widely scattered, the organisation will need to reflect on why this is. However, if the responses are predominantly in a single column, the following descriptors summarise the organisation's CIRM maturity:

Low: The processes or arrangements in place for CIRM are the minimum required for compliance and are given low priority. As a result the organisation is at high risk of operational, financial and reputational damage caused by cyber insiders for which the Board is accountable.

Medium Low: There are appropriate processes or arrangements in place for managing the business risk arising from cyber insider incidents but these are purely reactive. As a result the organisation is at moderate risk of operational, financial and reputational damage caused by cyber insiders for which the Board is accountable.

Medium: There is a consistent, defined, organisation-wide approach to CIRM which addresses a wide range of influencing factors but which is not properly integrated with other aspects of corporate risk. As a result the organisation is still at some risk of operational, financial and reputational damage caused by cyber insiders for which the Board is accountable.

Medium High: The organisation manages CIR proactively, actively monitors precursor indicators and fully engages staff in responsibility for security. As a result the organisation is at low risk of operational, financial and reputational damage caused by cyber insiders for which the Board is accountable.

High: CIRM is fully integrated into the organisation's working practices and the organisation is committed to continuous improvement. As a result the organisation is at very low risk of operational, financial and reputational damage caused by cyber insiders for which the Board is accountable.

CONCLUSION

However it is used, the CIRM Matrix should enable organisations to understand better their exposure to the harmful acts which their own employees may carry out, whether intentional or unintentional and malicious or non-malicious. This understanding should enable a programme of improvement in order to mitigate risk and thus protect the organisation. ■

REFERENCES

(1) CYBER INSIDERS – A BOARD ISSUE, Cyber Security Review, Summer 2014, Available at: https://issuu.com/deltabusinessmedialimited/docs/cyber_security_review_summer_2014/63?e=6269486/8102039 (Accessed 28 October 2016).

(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: 28 October 2016).

(3) PRE-EMPLOYMENT SCREENING, A GOOD PRACTICE GUIDE, EDITION 5: JANUARY 2015, Available at: http://www.cpni.gov.uk/documents/publications/2015/pre-employment%20screening%20edition%205%20-%20final.pdf?epslanguage=en-gb (Accessed: 28 October 2016).

(4) ONGOING PERSONNEL SECURITY, A GOOD PRACTICE GUIDE, EDITION 3: APRIL 2015, Available at: http://www.cpni.gov.uk/documents/publications/2014/2014006-ongoing-personal-security.pdf?epslanguage=en-gb (Accessed: 28 October 2016).

(5) HOLISTIC MANAGEMENT OF EMPLOYEE RISK (HoMER), 2012, Available at: http://www.cpni.gov.uk/documents/publications/2012/2012021-homer.pdf?epslanguage=en-gb (Accessed: 28 October 2016).

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, a Member of the Register of Security Engineers and Specialists and an Honorary Fellow at Warwick University. As an independent consultant, Chris advises international companies and government organisations on how to mitigate the risk of harm caused by their own employees.