RISKADVISORY

BUSINESS RECOVERY TOOLKIT

Protective security risk audit

Framework questionnaire – An exercise in identifying enterprise wide security risks and vulnerabilities.

Questionnaire fundamentals

We have developed an iterative process when dealing with protective security and risk management based on three fundamentals.

Firstly, we take a risk-based approach where:

Security Risk = Threat x Vulnerability x Impact.

For a Threat to be credible there must be capability and intent, and as Threat is generally external it is often beyond control. However, Vulnerability and Impact are absolutely controllable.

Second, we believe that effective protective security is dependent on three interdependent components. We call this converged security, the three components being:

- Physical security (gates, guards, access control);
- Personnel security (staff screening, insider threat); &
- Cyber-security (systems, architecture, firewalls, testing and exercising).

Thirdly, we view Threats, Vulnerabilities and Impacts through the following five lenses:

- People and Culture
- Leadership and Governance
- Technology
- Policies and Procedures
- Data and Information Management

Recognising that security risks are both dynamic and adaptive, we find that basing our approach on the three fundamentals listed about gives us a rich picture and a trusted methodology to reduce security risk.

Responses and Scoring

These questions are broad in nature and you are requested to select a score between that most closely reflects your situation.

1. No / Poor or non existent
2. No / Currently under review
3. Yes / Needs improvement
4. Yes / Excellent

General Security Overview

General security describes general measures, policies, procedures and awareness of security related matters across the organisation.

1. Does your organisation's leadership receive a regular, relevant and reliable feed of threat information (internal and external threat), which it can monitor over time?

2. Is there ongoing assessment of the effectiveness of current controls in managing general and security risk within the organisation?

3. Is the organisation aware of current and future threats to the organisation and individuals?

4. Are policies, procedures and strategy in place within your organisation for identifying and allocating responsibility and ownership of risks?

5. Is there experience at a senior leadership level within your organisation of risk management and strategy?

6. Are procedures in place for evaluating and reviewing risk across your organisation as the organisation develops and the threat landscape changes?

7. Are there levels of risk compliance or regulations that your organisation are currently committed to?

8. Does your organisation have a clear set of values or policies which incorporate the importance of security?

9. Does your organisation have a culture of openness and transparency whereby employees know where to go if they have a concern about any activities (whistleblowing process)?

10. Does your organisation openly and continually communicate risks where appropriate? Are your organisation's stakeholders empowered to communicate on risk related matters?

11. Are there existing communications and information security procedures and policies in place?
12. Does the leadership team travel internationally more than once a month?

Physical security

Physical security describes security measures that are designed to deny unauthorised access to facilities, equipment and resources and to protect personnel and property from damage or harm.

1. Has your organisation established/specified the physical security standards for their property portfolio in line with the current threat assessment?
2. Are appropriate physical security measures (fences, barriers, vehicle mitigation, alarm systems, access control, CCTV, guards and incident management systems) in place across your estate currently?
3. Are there clearly defined roles, responsibilities and reporting mechanisms, especially for outsourced security measures/systems
4. Are physical security risks currently monitored and reported within your organisation?
5. Have training initiatives taken place within your organisation in relation to physical security matters, for example; a suspect package or vehicle at reception, discovery of an intruder in a senior managers office?
6. Is there a physical security risk register?
7. Are physical security policies owned, reviewed and updated?
8. Does your organisation have visitor procedures in place currently?
9. Does your organisation have communications security procedures in place?
10. Are office emergency procedures and policies in place for events such as fire, lock down, safe room, suspicious package / bomb threat?
11. Are the right policies, training programmes and cultural norms in place to ensure that employees and suppliers understand and respond to the security threats they may encounter including in their home environment?
12. Are employees and suppliers aware of their security responsibilities to each other and the organisation?

Personnel security

Personnel security is a system of policies and procedures which seek to mitigate the risk of workers (malicious insiders) exploiting their legitimate access to an organisation's assets for unauthorised purposes.

1. Does your organisation’s leadership consider personnel security and insider risk issues when it makes major strategic decisions?

2. Does your organisation’s leadership incorporate insider risk into operational decision making at every level of the organisation?

3. Does your organisation’s insider risk management strategy include contractors and partners as well as staff, and does it recognise the importance of both deliberate and accidental acts?

4. Is the effectiveness of insider risk management tested and measured (external audit, penetration-testing, regulatory standards?), and is there a single person responsible for this?

5. Does your organisation have measures in place to monitor changes in the level of insider threat?

6. Is there a thorough understanding in your organisation of the range of technical and other controls available to manage insider threat, and the practical, legal and technical implications of their use?

7. Does your organisation have a graduated approach to personnel security and insider threat management, using role-based security assessments and access controls?

8. Is there a cross-functional (HR, Legal, IT monitoring, Security etc.) group in your organisation with the skills to capture and assess insider threat information, and to oversee investigations?

9. Does your organisation monitor user activity on its systems to identify potential insider threat activity?

10. Does your organisation have a robust Joiners Movers Leavers process which enables it to know who is employed at any given time, and to manage their access to critical assets.

11. Does your organisation conduct appropriate suitability assessments of its staff and contractors at pre-recruitment/pre-engagement, and throughout the course of their employment?

12. Does your organisation have a strategy/programme for supporting the mental health of its employees, and identifying those experiencing stress or other psychological problems?

Cyber-security

Cyber security is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.

1. Is there a general awareness about cyber threats and how they manifest against an organisation or individual?

2. Has any member of the board managed or been part of a cyber incident (real or an exercise)? Has the team ever practiced or exercised a cyber incident?

3. Has your organisation's leadership team ever undertaken cyber, General Data Protection Regulation (GDPR) phishing / spear phishing training or exercising (either collectively, individually, or in previous employment)?

4. Does the team ever openly discuss cyber security in any meetings or discussions, either as an agenda item in a meeting or organically in conversation?

5. Does the organisation have any existing policies or procedures (including flowed down from external stakeholders) that are in place or need to be in place?

6. Do you have a nominated senior cyber risk champion? If not, do you have plans for one?

7. Does the leadership team avoid password reuse across systems?

8. Are there any external or third party requirements for mandated or required cyber policies or procedures to be in place?

9. Do your staff have an understanding of data that is critical versus data that is less critical to the success of the project? If so, is that data taxonomy documented?

10. Are your staff willing to alter their ways of working slightly to accommodate higher levels of encryption throughout the data storage and communication systems? Are the users willing to undertake minor adjustments to their ways of working to increase security and reduce risk?

11. Are there any data classification (official or otherwise) or handling instructions (again official or otherwise) placed upon your organisation's stakeholders from external third parties?

12. Does the leadership team predominantly work remotely?

GET IN TOUCH

Contact us now to find
out how we can help

+44 20 3073 9021
businessrecovery@riskadvisory.com
www.riskadvisory.com