RISKADVISORY

BUSINESS RECOVERY TOOLKIT

GET IN TOUCH
Contact us now to find out how we can help

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

Rapid Insider Risk Assessment

Scenario: Downsizing or liquidation

Triggered by Covid-19, your organisation might be considering either a dramatic downsizing or potential liquidation. Unless handled well, this could leave you vulnerable to insider threat.

1 Establish group of trusted stakeholders

Identify and vet (inc. OSINT) a group of trusted stakeholders from key business areas to lead the restructuring programme.

Take measures to ensure the group is motivated to participate in the process.

Design and establish an operating model for the group, including IT and comms to ensure the security of their activities

Duration: 2 days

Format: Interviews with retained staff, document review

Resources: Lead security adviser, 2 x security analysts.
Note: resource involved in vetting will be separate from advisers.

2 Identify critical assets and 'worse case' insider scenarios

With the trusted group, identify critical assets that need to be protected, realised and/or decommissioned.

Conduct interviews with trusted group to identify business areas where insider risk is likely to be most elevated.

Consider who has the skills, access and motivation to damage/steal critical assets.

Examples of critical assets:

- Customer data
- Sensitive corporate data

Duration: 1 day

Format: Internal workshops

Resources: Lead security adviser, 2 x security analysts

3 Test insider risk scenarios

Run blue and red team exercises with trusted group to test 'worst case' insider scenarios.

Identify causes and pathways most likely to lead to damage to critical assets.

Assess likely effectiveness of existing controls.

Identify flashpoints in the company closure / restructure process most likely to increase insider risk.

*Examples of impacts to critical assets:

- Theft or leaking of personal data (e.g. customer booking records)

- Deletion of sensitive information for investigation (e.g. C-suite office records)

Duration: 2 days

Format: Coordinated delivery with retained staff

Resources: Lead security adviser, 1 x security analyst

4 Advise on mitigation measures

Provide guidance on human behaviours and technical activity most indicative of insider intent.

Advise on sequencing of corporate actions to reduce motivation and opportunity for insider acts.

Advise on content and sequencing of comms to reduce levels of staff anxiety.

Suggest technical controls to deter or detect behaviours most associated with 'worst case' insider scenarios.

Leverage existing tools and advise on new ones to detect insider behaviours.

Duration: On demand

Resources: Security analyst, lead security adviser

5 Monitor and advise

Provide ongoing assurance of 'trusted group' and the information it generates e.g. through OSINT checks.

Provide the group with ongoing advice on specific insider risks or incidents as and when they occur.

Implement a triage and escalation process for security incidents.

Convene periodically to re-evaluate insider risks and monitoring measures.