National Protective Security Authority

CASE STUDY

Illustrative Role-based Risk Assessment case study in a Small Medium Enterprise

This fictional case study has been designed to show how you might approach and collate the information during an insider Role-based Risk Assessment process.

This company has c500 people. It is a manufacturing company, based in the UK, but distributing worldwide. There are some UK based competitors and recently the overseas market has started to develop this process.

The company is in a business park with other similar manufacturing companies, on the edge of a large urban city. The workforce is mainly recruited from the local areas.

The company has two main focuses – the manufacturing process and the sales department, and recently formed a small research team looking at future technology as a result of the increased overseas interest in the manufacturing process.

The company have asked the security manager to develop an insider risk register. Due to the size of the organisation the security team have identified that an organisational-wide approach will be appropriate.

Steps to take:

1) Identify the company assets
2) Categorisation of assets
3) Threat identification
4) Conduct Role-based Risk Assessment

Company Asset identification and classification

Think about the functions of the business – the main production line, the sales department, and the corporate support functions (such as HR, finance, legal, IT support, facilitates management) for each function.

A good starting point is to “walk through the day”, get your stakeholder group to think about what they interact with as part of a normal day in the office.

For example: you are heading into work:

- where is it (eg single location, or a floor in a shared office site)?
- Do you need a pass to enter the building (either to access the building or to show the guard)?

What next:

- what do you log into e.g. a company computer and corporate systems, which can be accessed through your laptop and the fixed IT computers?
- use phones (mostly mobiles) ?
- use an email system and access corporate files?
- it might be that you are on the production floor and working in a particular area:
- how does the production line run – what equipment is there?

Who do you interact with:

- Other teams in the office,
- external stakeholders,
- clients,
- third party suppliers,
- contractors, etc?

Once you have a good understanding of how the organisation works you can start to think about specific assets – such as the building and equipment, the personnel and identify which elements you would consider critical to the continuity of service/production. This enables you to build an asset register (see chart below for illustrative purposes).

You will need to think about how you classify and protect your finished asset register – NPSA recommends that access should be on a need-to-know basis only (for example, your business continuity teams, security teams and relevant senior executives).

ASSET REGISTER

Organisation		Your company name			
Asset	*Type*	*Function*	*Owner*	*Critical Y/N*	*Strategic threat actors*
Main building	Physical	Location where all business takes place (manufacturing/production, sales, corporate functions and research team)	CEO	Y – no fallback options for the manufacturing stages – corporate functions and sales can work remotely	Criminal damage (external)
Production line	Physical	End to end production line	Director Ops	Y – fixed floor plan purpose built for the process – no current fallback option	Espionage/ Insider activity
AI robotic arm	Physical	Specialist equipment recently installed to speed up production	Director Ops	N – production line can be maintained without AI – albeit slower	Espionage/ Insider activity
IT Server cupboard	Physical	Supports the functionality of the company IT infrastructure	Director Corporate	Y - IT powerhouse of the business - there is a backup but never tested	Espionage/ Insider activity
Computers/ phones	Physical	Office equipment (mainly used by sales and corporate functions)	Director Corporate	N – fallback options available albeit at cost	Espionage/ Insider activity
Production staff	Personnel	Staff working on the manufacturing floor	Director Ops	N – easy system to operate, with minimal training,	Espionage/ Insider activity
Engineering	Personnel	Production line maintenance	Facilities Management	Y – currently an old system requiring specialist in-house engineering knowledge – only one current engineer with this	Espionage/ Insider activity
Sales team (UK)	Personnel	UK focused sales team	Director Sales	N - although a small team, all multi-tasking with access to all records so can take a loss/reduction in numbers.	Espionage/ Insider activity

Sales team (Overseas)	Personnel	UK based but working exclusively in overseas marketing	Director Sales	N - as above - although each team member responsible for one overseas geographical area and guilt up good relationships - can be re-built but would take time	Espionage/ Insider activity
IT support	Personnel	Contracted in-house (1pax) and remote team (call centre)	Director Corporate	Y – potential single point of failure with only 1 in-house IT support function	Espionage/ Insider activity
Corporate team (HR, finance etc)	Personnel	"S-File" systems as well as Microsoft operating system - also linked into the phone network	Director Corporate	Y - although only certain areas of the S-file system (such as the Payroll and HR database. Is the main operating system, with contracted IT support	Espionage/ Insider activity
HR & Payroll Database	IT	Part of the S-File corporate network	Director Corporate	Y - holds all staff details (personal) as well as payroll data. GDPR requirements	Espionage/ Insider activity
Customer Database	IT	Part of the S-File corporate network	Director Corporate	N - although holds details of all customer base - including payment schedules/reductions, contact details there are soft and hard copies held with the soft copies updated monthly	Espionage/ Insider activity
Research data	IT	Part of the S-File corporate network	Director Ops	N – not yet in early stages but recognition this could change given research direction	Espionage/ Insider activity/Sabotage
Production line software	IT	Stand-alone purpose-built operating system, not linked into anything other than the new AI robotic arm	Director Ops	Y - old bespoke system no commercially available substitute	Espionage/ Insider activity/Sabotage

Threat assessment

Think about what threats your company might face – develop relationships with your local crime prevention officers, counter-terrorism security officers, join any local security groups (or set up one) and make use of the UK national technical authority (NCSC and NPSA) websites so that you are threat informed.

Consider:

- External threats:
  From the profile of the company threats from terrorism seem unlikely, although in an urban city they are away from crowded or iconic places/transport hubs, they are not manufacturing a product that would be of interest to single issue or domestic extremism. There is a potential for hostile state activity – the company is selling the product overseas and is aware that there is current interest from overseas companies in developing the product themselves. Commercial espionage is also of interest given the small number of UK companies making this product and the need to remain competitive. There are no reports of serious organised crime, but the local crime data suggests they are in an area of deprivation with vandalism and thefts occurring regularly, particularly late at night.

- Internal threats:
  Small company with a low turnover of staff but a recent round of redundancies has led to resentment – particularly with the use of technology to replace people-based roles. The sales dept is very competitive and staff are regularly headhunted by their competitors. The company has not suffered any major security incidents in the last five years, but there have been IT related issues with company information being sent to the wrong people. Internal investigations have been carried out suggesting it was accidental

- Threat profile:
  Espionage (potentially state sponsored and commercial), criminal damage and insiders (current level of resentment, and unintentional activity)

The company is right to carry out a Role-based Risk Assessment as their current threat profile has identified threat actors that are known to use insiders to get the information they want.

Role-based Risk Assessment

Using the main types of insider risk think about specific insider activities that make use of any critical assets you identified e.g. sabotage of a production line, unauthorised disclosure of a database or staff details.

Think about whether these can be deliberate acts or unintentional and assess l**ikelihood** of that event occurring in the organisation and the **impact** for each.

Remember to think about whether any existing countermeasures are in place and whether they are adequate to reduce the impact.

For each identified risk think about who has access – members of staff, contractors, visitors, supply chain etc). The table below illustrates this methodological approach.

Asset/Team	Widget PLC						
Strategic threats	Commercial and state sponsored espionage (technology/financial), insider activity (both unintentional and malicious), criminal damage						
Strategic insider activity	**Insider risk**	**Likelihood (1-5)**	**Assumptions**	**Impact (1-5)**	**Assumptions**	**Identified roles**	**Priority (HML or 1-4)**
1. UNAUTHORISED DISCLOSURE							
	1a) Member of staff sends the customer database to a competitor (UK)	4	Access to database not compartmentalised, no staff IT training or security awareness, has happened before but no remedial actions taken, no current IT measures to audit database usages	2	Reputational damage and potentially loss of client but consider the product is marketed competitively that no lasting impact	Entire sales team, corporate director, IT support, Op's director	**2**
	1b) member of staff sends the customer database to a competitor (overseas)	3	As above - but lower likelihood as fewer people have overseas contacts	3	As above - but concerns that overseas markets are developing their own processes which would then provide them with potential client information	Overseas sale team, Corporate and Ops Directors, IT support and research team	**1**
	1c) member of staff invertedly attaches client details to email to another client	4	Has happened before - fortunately no damage to organisation, no obvious evidence of any mitigations put in place as a result. No real training programme in place for good IT security	2	Reputational damage and potentially loss of client but consider the product is marketed competitively that no lasting impact	Entire sales team, corporate director, IT support, Op's director	**2**

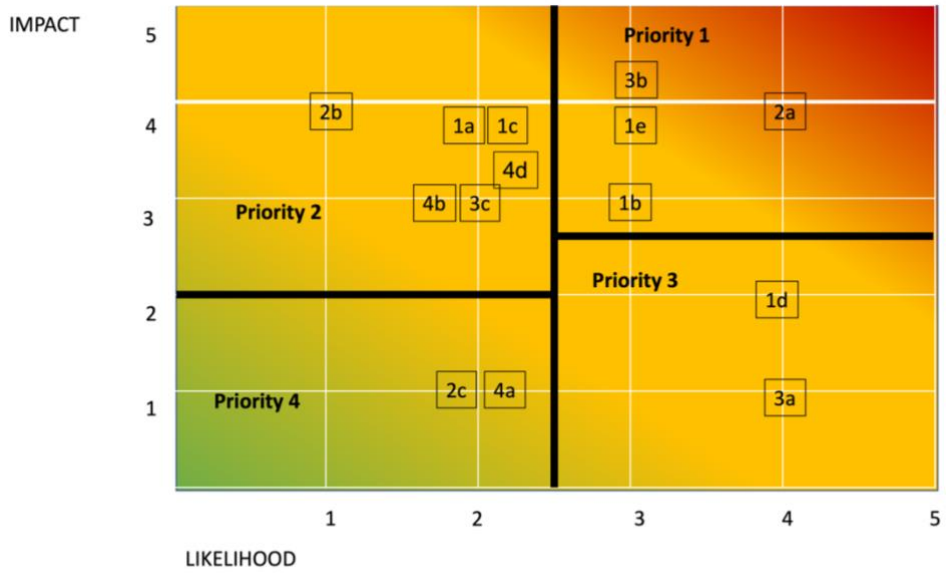
	1d) Member of staff sells staff details (from the HR database)	2	Small close knit HR team, only have access to parts of the database rather than the whole. Would need specialist IT knowledge to extract the data - although it could be printed off in hard copy. Staff have annual GDPR training	4	GDPR consequences (fines), loss of confidence by staff to hold data securely	HR and Finance team, Corporate Director, IT support	**3**
	1e) Member of staff sends research data to a competitor	3	Research team newly formed - not sure of remit/direction or continuation of funding, being headhunted by both UK and overseas competitors	4	Team looking at new ways of production - cutting edge, now ahead of the competitors, would seriously damage the viability of the company if this material was compromised	Research team, IT support	**1**
2. PROCESS CORRUPTION/ SABOTAGE							
	2a) Member of staff deliberately damages the production line halting work for several weeks leading to a loss of income for the company	4	Current resentment in the production staff team due to recent redundancies - management desire to modernise and automate more parts of the process. Competitors keen to see the company. No floor plate controls in place - everybody has access. Lines are kept ready overnight. No access controls to monitor out of office access	4	Production line currently old - bespoke rather than off-shelf technology, replacement parts would have to be built from scratch	Potentially all staff (production and corporate, facilities management - cleaners), visitors, contractors, and supply chain	**1**
	2b) Member of staff deliberately damages the AI automation equipment,	4	As above - high level of resentment within team, believe the introduction of AI further increases likelihood of redundancy.	1	AI only involved in a small part of the production line now - currently can be replaced by a member of staff	As above and the AI technician	**2**

	2c) Member of HR creates a false employee record to pay bogus wages	1	All HR staff have ability to create records but need a senior authorisation to finalise record (so collusion would be required). As it's a small team most of the office know each other (not a lot of contractor or temporary hires) to disguise a bogus employee	2	Financial consequences, but would not be a long-term damage, May result in a criminal investigation and advisers press but considered to be manageable.	HR staff	**4**
3. THIRD PARTY ACCESS							
	3a) Member of staff provides access to the site for a third party to enter the production line and damage it	1	would need to be outside of core hours otherwise the third party would be seen, however, there isn't a challenge culture and staff are used to seeing visitors wandering around the floor	4	Production line currently old - bespoke rather than off-shelf technology, replacement parts would have to be built from scratch	All staff	**3**
	3b) Member of staff provides computer password giving access to S Files including the client database and research data to a competitor	3	Production staff (due to current morale and resentment - but who have logins for training and HR requirements), but potential for any member of staff possibility through social engineering to provide this information	4	Lack of compartmentalisation of S files, poor IT security control and audit, Files can be downloaded and printed with ease	All staff	**1**

	3c) Member of staff has their bag stolen leaving work with their laptop and password in it	3	Has happened before - high crime in the area including theft - laptop has been recovered with no evidence that it has been logged in and used. IS an awareness campaign running to remind staff to be vigilant when leaving the office particularly during dusk and dawn. Police are currently doing drive bys at key times as a deterrent - but expect this is a short-term approach. Possibility that laptop could be stolen to order by a competitor	2	Although individual impact is high, for the company it is manageable. No evidence that laptop would be passed to a competitor. However, if the laptop is stolen to order the impact would be higher especially of it was the research data that would be exploited (keep under review)	All staff	**2**
4. FINANCIAL IRREGULARITY							
	4a) See 2c)	1	see 2c	2	see 2c	see 2c	**4**
	4b) IT Support falsely bill for extra hours	3	IT team (all contractors) working on an hourly basis (as and when needed) have an upper limit/budget before checks put in place but otherwise little accountability of hours worked. Hours individually submitted and signed off by Corp director - but at present no checks made	2	There is a financial limit which lowers impact. As with 2c) could be a criminal investigation and adverse press - considered to be manageable. Currently looking at online IT solution that would provide auditing function	IT contractors, Dir Corps	**2**

	4c) Member of staff sells spare parts of the manufacturing line to competitor halting production	2	Most of the equipment is bespoke so not necessarily fit for other competitors. Stores are under the control of the engineering team and generally locked away. Regular stock takes taken to ensure continuity of service should a replacement bit be required	2	Links into potential sabotage in that the kit is bespoke so no off the shelf response available	Engineering team	
	4d) Member of staff sells spare parts of the manufacturing line to overseas competitor halting production – but also providing blueprint for overseas manufacture	2	Stores are under the control of the engineering team and generally locked away. Regular stock takes taken to ensure continuity of service should a replacement bit be required. Stocktakes always a two-person audit	4	Long term financial implications as overseas competitors can use this to help design/build their own production line taking away potential customers	Engineering team	
5. VIOLENCE/ PHYSICAL ATTACK							
	Considered as part of the wider insider risk but at this time assessed to be unlikely						

Once this is completed you can now plot the risks on the heat grid – check that there doesn't seem to be any anomalies (outlier risks that seem at odd with the rest) and decide how you want to prioritise the risks for action depending on the company's risk appetite and available resources.



Analysis, Action and Review

You can see from the heat grid that there are clusters of similar risks. You can use this information to feed into the company's strategic risk register. For example, there are currently multiple opportunities for the unauthorised disclosure of information to occur – both accidentally and deliberately. Feeding this into the strategic risk register provides valuable information to the Board to act on and support mitigating security initiatives.

Seeing how risks are clustered can also help focus any mitigations you put in place that may positively affect several risks – reducing likelihood/impact. For example, introducing a security behaviour change campaign focusing on good IT security practices, in tandem with improving the audit controls on the databases, may reduce the likelihood of accidental and deliberate unauthorised disclosures of information. Introducing an access pass system for the manufacturing floor may act as a deterrent to stop sabotage of the equipment. See the NPSA insider risk pages for more mitigation information.

When mitigations have been put in place (and embedded in the organisation) it is important to review your risk register to see what changes have occurred.