Strategic Threat Evaluation – considerations for your information security management system (ISMS) business case.

Evaluate each of the areas below and estimate the consequences as part of your strategic threat evaluation. How long you spend on the evaluation is up to you. It should be based on the risks and rewards facing the organisation and the need to justify the case for investment for your powerful stakeholders.

	Threats	***Considerations for your business case***	***Value / measure example***	***Your estimate?***
1	Existing (especially powerful) customers no longer believe you can be trusted so avoid renewing your contracts	What percentage and financial value of your customer base is powerful enough to demand an ISMS they can trust (e.g. independently certified or at least more visible than what you have today?)	% of customers powerful enough to force change £ contract value of powerful customers £ contract value of all customers	
2	Cost of sale increases as more prospects seek assurances from information security and privacy practices Assume smart powerful buyers will not entertain suppliers without recognised ISMS standards	How much more will your selling costs increase to demonstrate you can be trusted? (e.g. extra sales hoops to jump through, more paperwork and audits to undertake)	% increase in cost £ increase in direct cost of sale per opportunity £ indirect increase in total cost from receiving fewer opportunities to bid on	
3	Go-to-market partners no longer believe you can be trusted so avoid promoting and reselling your products and services	What percentage and financial value of your channel to market is powerful enough to demand an ISMS they can trust?	% of channel partners £ partner revenues	
4	Your important suppliers are poorly managed by you or unable to demonstrate they can be	What are the threats from suppliers not performing or breaching	£ value of assets managed or	

	trusted and you face consequences from their performance failures	confidentiality, integrity or availability of information?	accessible by suppliers % and £ of customer contracts likely to be lost	
5	Powerful suppliers actually consider you too big a GDPR risk to process personal data for, or increase prices to reflect their risk appetite on supply	What percentage of your data processors may consider your approach to GDPR a risk for them given regulation change?	£ supply side price increases for risk % of business at threat of non-supply/ no alternatives	
6	Loss of valuable information from a breach affecting future trading capability: financial, personal, IPR, contracts etc	Consider the type and value of your organisation's information assets and if appropriate those it is safeguarding for others (avoid double counting from other rows above)	£ direct financial loss (e.g. breached bank accounts) £ cost to rework valuable IPR lost £ loss of any advantage in trading (e.g. commoditisation from imitations arriving or rareness of offer being eroded) £ direct loss of commercial contracts affected	
7	Customer, partner, supplier civil suits as a result of contract failure and breach	Customer, partner, supplier civil suits as a result of contract failure and breach	£ direct cost of loss/consequential loss £ cost of legal services	
8	Regulator and legislator fines	GDPR being the most obvious with up to €20m or if higher 4% of global turnover at risk	£ fine £ cost of appeals/legal work	
9	Reputational consequences leading to financial losses	The impact on your brand and ability to do what you did before	Contract losses not considered above Share price losses	

			£ PR recovery costs £ increase in marketing spend £ increase in sales costs	
10	Remediation costs following incidents	The direct cost and opportunity cost from addressing incidents that arise	£ cost from number of incidents x cost of incident resolution £ loss of staff time/income in not addressing day job	
12	Insurance costs and other related risk premium increases	The cost of insurance is growing because of cybercrime and privacy anyway and may grow further faster if you have a claim	% increase in existing premiums and £ cost £ of new insurances required e.g. cyber insurance without evidence of any ISMS certification	
	Summary impact from Threats	***£*** ***Notes….***		

This is one of the templates provided in good faith to help you consider and evaluate the return on investment (RoI) from an Information Security Management System (ISMS).

If you would like more help with building your business case for an ISMS or are ready want to get your ISMS.online then please contact us at www.ISMS.online and organise your consultation.