Top Ten Tips: Cyber Security / Mitigation of Attack

1	Proactive Risk Management	Make sure you understand where risks could arise, and what level of risk you are prepared to run. Document your decisions around your level of risk appetite.
2	Overconfidence or lethargy: "we won't be caught"	Do not assume that all your organization is not likely to be attacked - No business, however large or small, is immune to data breach and or cyber attacks. There is evidence that small to medium size organisations are at a higher risk as they don't invest in data and cyber security measures to mitigate the risks - often due to budgetary considerations.
3	Fortifying 3rd party supply chain	Threat actors, aka the Cybercriminals, frequently target small organizations in order to gain access to larger ones, through the 3rd party supply chain - the biggest source of data breach and cyber attacks. Ensure that you have checked the security protocols that your 3rd party alliances have in place.
2	Robust Incident Response Readiness	No organization, however large or small, is immune to data breach and or cyber attacks so everyone should be prepared with an incident response plan, kept in a secure place and that is accessible
3	Rapid Response Escalation	Do not delay when there appears to be some anomaly - and ensure that your staff all understand that need to alert senior management as soon as they suspect an attack. Have a clear escalation plan in place: who to contact and who to call
4	Expert Resources and Incident Response Team	Be prepared with the relevant expertise in place: technical response to minimize the effects of the attack and re build, law enforcement who can help predict the threat actors' next move and modus operandi, forensic investigation to assess the situation, negotiators in case of ransom demands
6	Strategic Communication Control	Ensure all communication is channelled through one source – both internal and external. A coordinated message is key. Notification to "data subjects", the 3rd party and the regulator may be required legally, but is key for maintain the organization's reputation
7	Navigating Cyber Insurance	Look at examples of where cyber insurance policies may or may not pay out, check what the common exclusions are and what the limits of cover might be - including sub-limits for incidents involving cyber extortion (ransomware)
8	Cautious Ransom Management	Don't rush to pay a ransom demand just to get the business back on track: you may be subject to fines and other legal action if the threat actors are criminal or terrorist. Undertake Cost Benefit analysis and involve a professional experienced negotiator
9	Legal Accountability and Defense	All organizations have legal responsibilities to clients / customers / shareholders and this is never more in evidence that during a cyber attack

		There is a trend towards individual liability for CISOs and board members who are being held to account for the consequences of attack, and actions taken to prevent and / or recover from them Organisations need a legally defensible narrative to deal with regulation issues and litigation.
10	Comprehensive Cybersecurity Training	Ensure that all staff (including the board and senior management) are regularly trained. Without the senior management getting involved with cyber attack training, it is like rehearsing for a show on Broadway with only the understudies: on the first night the lead actors will not be ready