RISKADVISORY

Insider Threat - A Legal Perspective

Cyber security is currently a hot topic, but there is a risk that by concentrating exclusively on the external threat, many companies overlook a real danger within their business.

Risk Advisory views protective security as encompassing three interrelated domains: cyber security; physical security; and personnel security. The latter area encompasses personnel screening and the insider threat.

The core value of most businesses is held within (1) its technical know-how, (2) customer (and to a lesser extent, supplier) databases, (3) bespoke contacts, and (4) price structure. Those inside the company with authorised access to this sensitive data are often the people best placed to exploit the value of these assets to the detriment of the business.

An exclusive focus on outward-facing cyber and physical security, without considering the need for effective internal personnel security, exposes the business to considerable risk.

Two case studies bring this threat to life. These case studies are both true, with identities redacted.

Case study 1: Company A - Logistics and personnel services supplier

Company A is a substantial business supplying logistics and personnel to domestic and foreign (mainly US) military. Their IT systems were sufficiently robust to detect potential misuse of data by a senior manager, who was downloading and copying client lists, contracts and price structures. The activity could be tagged to the specific individual, dates, times and classes of material.

This material was being forwarded to external sources, including a counterpart in a competing business, and it appeared that the intention was to gain commercial advantage through insider knowledge.

The evidence was sufficiently compelling to enable lawyers to obtain a Search Order from the High Court, authorising entry of the homes of the senior manager and his counterpart and seizure of relevant electronic and hard copy evidence.

The order was executed at both locations simultaneously, to avoid the possibility of evidence being destroyed or hidden through them warning each other. In each case the search was supervised by an independent solicitor, and the electronic search conducted by an independent IT expert who imaged every electronic device on the properties.

The electronic data was removed to a secure evidence store, and keyword searches undertaken to identify relevant evidence. The evidence collated was sufficient for HCR to return to Court and obtain further orders (known as "Springboard relief"):

1. Forbidding the two parties from contacting named individuals and entities for a specified period
2. Compelling the two parties to deliver specific documents to Company A, delete all electronic copies, and allow access to Company A's IT experts to verify deletion
3. Compensation to Company A for losses and costs sustained, totalling over £500,000.

Case study 2: Company B - List X supplier to UK Ministry of Defence (MoD)

Company B is a List X supplier of technology to the UK MoD. They detected a potential misuse of data by a senior manager, however despite robust cyber-security against external threats the internal procedures and safeguards were virtually non-existent. Access was not restricted or password protected, USB's and devices were pooled and shared, and activity could not be tagged to individuals, dates and times.

In this case legal advice was not to apply for a Search Order, thereby saving significant wasted cost as Courts will only authorise a dramatic invasion of privacy in exceptional cases and many applications are refused, leaving applicants with large, unrecoverable legal bills. Similarly, legal advice was against seeking a Springboard injunction, as without the evidence, the financial risk was too great.

Company B was not sure whether to report the security breach to the MoD, and legal advice was a categorical yes. If an unreported breach was discovered later, they risked permanent loss of List X status leading to the probable loss of the business.

HCR liaised with the UK MoD police, who were persuaded to use their own powers of search and seized evidence at the home of the senior manager; the recovery of all of Company B's confidential information prevented it from reaching the competition and saved the business.

Lessons learned

The case studies above highlight some factors that organisations should consider when it comes to the insider threat:

- Where possible avoid shared devices, restrict access on a need-to-know basis, all individuals should have password protected access, all activity should be tagged and recorded, and external forwarding or copying tightly controlled
- All employment contracts must define breach of the processes listed above as gross misconduct, justifying immediate dismissal with extensive post-termination restrictions
- External parties who have engaged in unlawful competition do not escape liability. The emerging economic torts (including inducement of contract breach and conspiracy to injure) enable companies to seek protection against these external individuals and entities as well
- Obviously every business should be mindful of the potential cost of these processes. In the first case study above, the search order cost £15,000 to obtain and a further £25,000 to execute. The total cost of Company A's case to trial was £150,000. An order for recovery of costs is only as good as the defendant's ability to pay
- Often the potential cost is a bar to a wronged company seeking protection. That can be avoided by proper commercial insurance, particularly Legal Expenses Insurance ("LEI"). But beware as not all LEI is the same so be sure to take legal advice
- Finally remember that all law firms are not the same either. Experience of these issues is essential. For example a typical reaction of many lawyers presented with the Company A case study might be to send a threatening letter, which would have been highly counterproductive and could have destroyed a valuable business.

The lawyers acting in both cases were HCR (Harrison Clark Rickerbys). Risk Advisory's Intelligence and Security practice advises businesses in all areas of security to help protect their people, assets and brands.