RISK MANAGEMENT CONSULTANCY

Information management

Case study:
corporate resources hijacking

The Challenge

An online retail business owner suspects two of his key employees of fraud. Several clues led him to that conclusion but there was a lack of evidence. For some time the working atmosphere around the office was real tense in their presence but suddenly lightened-up when they were not around. When one of the employees started holding back information critical to the business, the owner decided to call upon professionals to solve the issue.

Asia Global Risk solutions

A forensic expert was dispatched on site to perform a forensic copy of the workstation of both suspects in presence of the business owner and a notary. Analysis of the data showed that both were working on the design of a new online retail platform intended to compete with the client on one of his key product range. It was obvious that most of their time in the office was spent on this new platform and that they were transferring most of their normal workload to colleagues. The key information held back from the business owner by one of the suspect was also recovered. A plan was quickly prepared to ensure the continuity of the business after the two employees were dismissed. That plan included the taking over by the management of critical information systems through AGR shortly before the dismissal and until the transition was completed.

The impact

The client was able to dismiss the two employees for breach of contract based on the evidence collected. The evidence was strong enough to discourage either employee to even attempt litigation against our client. The client did not have to wait until a replacement was found to dismiss them as AGR was able to take over some critical responsibilities during the transition time.

What the client valued

The fact that an intervention was arranged quickly outside office hours together with proper legal support and that the in-depth analysis gave definitive proof of the fraudulent activities. Our deep understanding of Information Systems allowed us to design and implement a transition plan for the remote management of some key information systems without any consequence for the business and with the full confidence that there would be no service disruptions.

RISK MANAGEMENT CONSULTANCY

Information management

Case study:
corporate fraud investigation

The Challenge

The regional management of a large industrial group suspects one of their senior managers to be involved in a large fraud operation. The senior manager is very well connected both inside the company, including with some IT staff, and on the local business scene. The client wishes to confirm the existence of an actual fraud and gather evidence without alerting the suspect.

Asia Global Risk solutions

The suspect had several electronic devices at his disposal that where assigned to him by his company. A pretext was arranged to obtain physical access to the devices and a forensic copy of the data was performed. To obtain further intelligence on the suspect's activity, a monitoring solution was also installed on all of his devices. The information gathered using these technical surveillance solutions was instrumental in breaking the case. A large operation was uncovered involving several suppliers and a factory that was set up to produce and sell copies of the client's products.

The impact

A major sidelining of all untoward elements inside and outside of the company took place following our report and this resulted in an increased competitiveness for the client on the market.

What the client valued

The fact that a monitoring solution was installed and monitored without the local IT staff being aware of it.

RISK MANAGEMENT CONSULTANCY

Information management

Case study:
Securing a high level meeting's proceedings

The Challenge

The client, a large multinational manufacturing concern, wants to hold a meeting in one of its major Asian offices and, because of the seniority of the company's officers present and the extremely sensitive trade and products related discussions, insists on having a pre-meeting physical and electronic audit as well as to guarantee an absolute protection against eavesdropping during the meeting to be held over a period of 2 days.

Asia Global Risk solutions

A thorough audit is conducted, using both electronic detection equipment and physical observation to determine whether listening devices, hidden cameras or any such equipment could have been placed in the relevant area by third parties. The audit also entails verifying if any distance eavesdropping (using laser equipment for example), IT hijacking or human interference are possible as well as defining the best possible set-up to jam all electronic signals during the proceedings. The meeting area is then physically secured until the proceedings start and jamming equipment is activated during the meeting while the area remain physically secured at all times.

The impact

The client was allowed to discuss major technical and strategic subjects impacting the region while being comfortably protected from any outside interference and competitors undue interest.

What the client valued

The in-depth understanding of the client's requirements as well as the technical know-how of AGR's officers, their reactivity in general and the fact that a senior member of the local team was left on duty throughout the duration of the proceedings to complement the client's security team.