Progress Test 2 Audio Script

Track 3

Interviewer: Gérard, what exactly is the difference between 'business intelligence' and 'industrial espionage'?

Gérard Desmarest: Well, the two terms are really very different because the first is entirely legal and the second is not. Business intelligence is the collection of information through any legal or 'open' source. So that could be through trade publications, business magazines, government organisations, specialist data sources, the internet or even just through straightforward observation. On the other hand, 'industrial espionage' is all about gathering intelligence by illegal methods. Now, there are various ways people can do that, by electronic surveillance, by stealing confidential information and, of course, by recruiting human agents from inside a business operation.

Int: How should businesses go about protecting their information?

GD: I'd say there are really two critical areas where businesses are particularly vulnerable; the first of those is through their information systems. It may be that a business hasn't protected its communication network properly. So it might not even know that critical files have been interfered with or have gone missing. So, protecting your information, how it is accessed and how it is exchanged – that's the first thing. On the human side, there are other dangers. People are not always honest and they may be prepared to communicate confidential information in exchange for something they want. You know, a competitor might try to influence or even hire a key member of your staff. So, you really need to have staff you can trust and that means being sure that what they are doing is in the best interests of the company. So, I'm afraid there are quite a lot of good reasons for companies to install software and systems to monitor the activities of their employees. It's sad to have to say that, but these days information is just too valuable.

Int: How would you advise an employee to be more aware of the danger of espionage?

GD: I would say that it's more a question of training than advising. I say that because most employees do not understand the techniques that outsiders can use to obtain information about a business. So, intelligence or security training can be very helpful because it's always easier for people to protect themselves once they know what they have to protect themselves against. You know, competitors can get a lot of useful information from employees just by asking the right questions at the right time. And an employee may not even realise that he or she is being manipulated. So, good, basic security training is definitely the first thing, and that's something that most companies don't provide because they don't know the risks that they are running.

Int: Can you give us an example of a company that you have advised and explain how you helped them?

GD: Well, I'm afraid I can't give you any names but, er, yes, I can answer that question in general terms. I mean, I've been involved in cases where we've been called into a company that had been the target of industrial espionage, and our job was to identify and locate the systems that had been installed. These were mostly quite sophisticated electronic devices which recorded telephone conversations and monitored meetings and then transmitted that information to outsiders. So, the first part of the job was to conduct a full security review and we did that at the

weekend when there was nobody at the company. And then once we'd done that, well, we advised the company's information managers on what they had to do to make sure that it wouldn't happen again. But, er, obviously I can't discuss the exact details with you – in my profession we don't give away confidential information, we protect it!