### Scenario

When the FBI approached ACME Enterprises with news that a Chinese man had been caught in possession of highly confidential commercial information from ACME concerning a failed billion-dollar bid, management was dismayed. They understood their information security controls were best-in-class and had no idea how the information had escaped but were determined to get to the bottom of the leak. With assistance from the FBI’s forensic experts, painstaking analysis of the executive information servers revealed a spyware infection that had never been seen before, hidden deep in the operating system. The antivirus software completely ignored it, and the antivirus company insisted the reason it had not been detected was that it was custom-written using strong encryption. The really shocking part of the incident was that nobody had picked up on this incident in the three years since the failed bid, not even the fancy intrusion detection system running on the corporate network. The CEO suddenly understood why ACME might have had such a run of bad luck in the market place: ACME’s competitors evidently weren’t playing fair.

### Questions and discussion points

1. Outline the information security concerns in this scenario.

2. The Chinese are frequently accused of cyber-espionage, but are they always to blame?

3. Imagine you are ACME’s CEO. What are you doing to do about this incident?
Model answers

Note: these are not meant to be definitive or comprehensive answers, nor are they legal or information security advice. We’re simply trying to help you discuss and learn from the case.

1. Information security concerns:
   - This is a serious malware incident
   - The infection was evidently sneaky, custom-written, well hidden, and lasted for years i.e. an Advanced Persistent Threat (APT)
   - It is possible that whoever was behind the attack has gained – and still has - unfettered access to ACME’s data and systems
   - Even if the specific piece of spyware is eradicated, they may well have placed backdoors or other malware that allow them to continue the attack indefinitely
   - ACMEs defenses have been breached and are clearly in need of improvement

2. Are the Chinese always to blame:
   - No – it’s not always the Chinese
   - There is reliable evidence that many countries are actively engaged in cyber-espionage
   - The Stuxnet incident, for example, was blamed on the US and Israeli governments
   - Many countries are actively recruiting/training IT professionals for cyber-espionage and counter-espionage, cyber-defense and/or cyber-offense etc.
   - In cyberspace, physical location or nationality is almost irrelevant
   - Aside from foreign governments, terrorist and criminal groups are using similar techniques, including custom-written malware

3. Potential CEO response:
   - Re-evaluate the risks
   - Examine systems and networks in depth for further infections, focusing on those holding, processing or communicating the most commercially sensitive/valuable information
   - Improve the security controls e.g. better malware detection, better network/system security (especially for the most sensitive/valuable information, e.g. compartmentalization, strong encryption), better security monitoring, better incident detection and response procedures, more evaluation of failed bids and other incidents to identify possible reasons, possibly a more proactive approach (e.g. seeding systems and databases with ‘honey tokens’, false/misleading items of data that, if disclosed or use by someone outside the company, must have been stolen; consider proactively evaluating the cyber espionage capabilities of commercial contacts, clients, partners etc. and adopting appropriate controls according to the assessed risks)
   - Learn the lessons – make changes (e.g. improve business continuity and contingency arrangements), don’t just think or talk about them!
   - Offer to resign i.e. accept personal accountability for the incident and the failures

Further information
This case study was inspired by news of an APT incident affecting Coca Cola. Browse the intranet Security Zone for more on APTs, malware, forensics etc. Call IT Help/Service Desk to report information security incidents, near misses and suspicions.