

Corporate Espionage: A Guide on How Businesses Behave Badly

Jake Cremin : 14-18 minutes

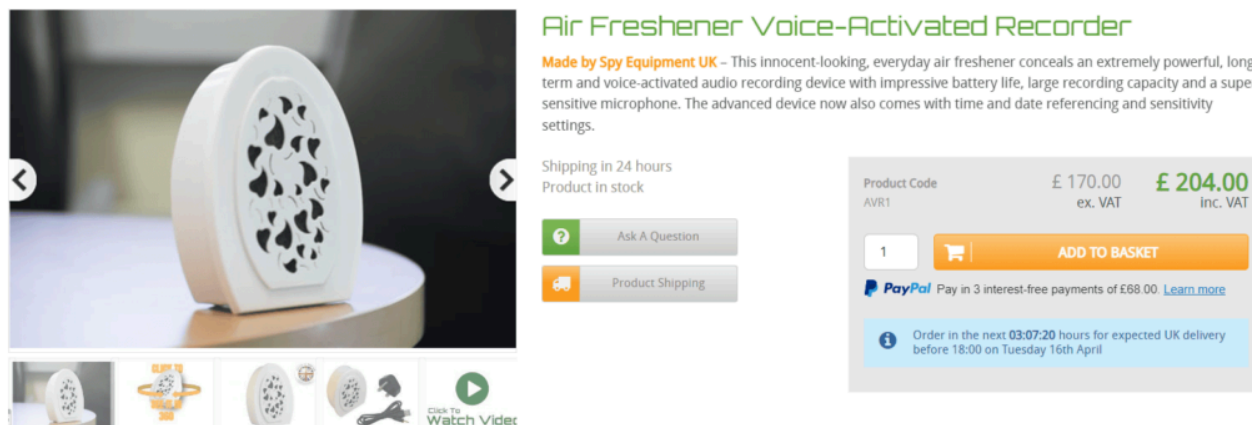
1.0 Introduction

Corporate espionage: While businesses focus on external threats like [hackers](#) and competitors, internal risks, often overlooked, pose significant danger to trade secrets.

From disgruntled employees to planted spies, 95% of data breaches have an internal origin. [\[source\]](#) Corporations invest significant resources into cybersecurity and legal protection only to be infiltrated from within the fortress they have built.

Corporate espionage is not unlike espionage practised by government [intelligence organisations](#). Corporate espionage is the sharp, clandestine and sometimes ethically dubious edge of business intelligence. Naturally, businesses spy on their competitors. Indeed, collecting information on business rivals is crucial to understanding the market and guides business strategy on everything from research and development through to trade policy. [\[source\]](#) What makes intelligence gathering espionage, however, is the means. From exploiting internal members of the workforce to planting backdoor spyware in processing chips, illegitimately gathering information provides rivals with a competitive advantage.

To keep market edge, corporations must be aware of espionage and safeguard against it. This article will explore what corporate espionage is, how to protect against it, and some key examples to be aware of.



The screenshot shows a product page for an 'Air Freshener Voice-Activated Recorder'. The main image is a white, oval-shaped device with a decorative pattern. To the right of the image, the product name is displayed in green. Below the name, a description states: 'Made by Spy Equipment UK - This innocent-looking, everyday air freshener conceals an extremely powerful, long-term and voice-activated audio recording device with impressive battery life, large recording capacity and a super-sensitive microphone. The advanced device now also comes with time and date referencing and sensitivity settings.' Below the description, it says 'Shipping in 24 hours' and 'Product in stock'. There are two buttons: 'Ask A Question' and 'Product Shipping'. To the right of the product image, there is a price section showing 'Product Code AVR1', '£ 170.00 ex. VAT', and '£ 204.00 inc. VAT'. Below the price, there is a quantity selector set to '1' and an 'ADD TO BASKET' button. Below the basket button, there is a PayPal logo and text: 'Pay in 3 interest-free payments of £68.00. [Learn more](#)'. At the bottom, there is a blue banner with a clock icon and text: 'Order in the next 03:07:20 hours for expected UK delivery before 18:00 on Tuesday 16th April'. At the bottom left of the product image, there are several small icons representing different features or accessories, and a 'Click To Watch Video' button.

A listening device or “bug” disguised as an air freshener. Perfect for eavesdropping on business execs sharing trade secrets. [\[source\]](#)

2.0 What is ‘Corporate Espionage?’

2.1 Towards a corporate espionage definition

The practice of illegitimately or illegally collecting confidential information without authorisation of its owner for commercial or financial purposes is referred to as corporate, industrial, economic, or commercial espionage. [\[source\]](#) Broadly speaking, corporate espionage splits between two distinct elements – physical and remote. The first involves physically accessing information stored on site or accessing people authorised to hand over the information. The second form involves remotely

penetrating a corporation through tricks or equipment, such as interception or recording devices. [\[source\]](#)

The US Federal Bureau of Investigation defines the following as “Economic Espionage”:

“Economic espionage is foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons ... his theft, through open and clandestine methods, can provide foreign entities with vital proprietary economic information at a fraction of the true cost of its research and development, causing significant economic losses.”

[\[source\]](#)

Examples of potentially sensitive “trade secrets” [\[source\]](#):

- Marketing strategies
- Pricing schemes
- Manufacturing assets such as processes, blueprints and CAD files
- Source code for closed source programs
- Original recipes

2.2 State-backed Corporate Espionage

Despite mostly occurring in the private sector, governments are not immune to corporate espionage, nor are they incapable of carrying it out. Over the past decade, corporate espionage has underpinned China’s strategy to lead the world in manufacturing. [\[source\]](#) Stealing trade secrets from western companies has become China’s official foreign policy.

Starting in 2015, the Chinese Communist Party set out ten high-tech industries in China would “focus on improving manufacturing” in order to reduce western dependence. [\[source\]](#) For the past decade, these ten industries highlighted have guided Chinese corporate intelligence collection priorities.

Corporate espionage scarcely prejudices between geopolitical friend and foe such is the financial and commercial draw. For example, Pierre Marrion, the former Director of the French Intelligence agency DGSE, stated:

“[Corporate espionage] is an essential way for France to keep abreast of international commerce and technology. Of course, it was directed against the United States as well as others. You must remember that while we are allies in defence matters, we are also economic competitors in the world.”

[\[source\]](#)

3.0 Technical Means, Methods and Equipment

3.1 Intercepting Ambient Conversation

Businesses do not store all their secrets on computer hard drives or in filing cabinets. In fact, some business secrets are not written down at all. However, all businesses eventually discuss secrets in conversation. That is where interception devices or listening “bugs” come in. People hide bugs within electronic devices and on their bodies to listen in and record confidential conversations. To illustrate, here are a few examples of bugs readily available to purchase online today:



GSM Phone Charger Listening Plug

Latest 4G version of this very popular mains-powered GSM listening device. A fully-functional USB mains adapter with a powerful GSM audio unit and built-in microphone with remotely switchable voice activation facility.

Shipping in 24 hours
Product in stock

[Ask A Question](#)
[Product Shipping](#)

Product Code PCL1	£185.00 Excl. VAT	£222.00 Incl. VAT
Package Options UK Style 3-Pin Plug - White (+£ 0.00)		
1	ADD TO BASKET	
Pay in 3 interest-free payments of £75.10 Learn more		
<i>Order in the next 03:01:45 hours for expected UK delivery before 18:00 on Tuesday 16th April</i>		

A bugging device disguised as an Iphone mains charger. Integrated 4G unit capable of receiving phone calls and therefore listening in real-time. [\[source\]](#)



GSM Calculator Listening Device

Made by **Spy Equipment UK** – Standard desktop calculator with inbuilt long term battery-powered GSM bug that is perfect for many applications. Ideal as a carry anywhere listening device, for inside the house, office, workshop or other indoor application. Very discreet and with excellent audio performance.

Shipping in 24 hours
Product out of stock

[Ask A Question](#)
[Product Shipping](#)

Product Code C4LG	£ 199.00 ex. VAT	£ 238.80 inc. VAT
This product is currently out of stock, please fill in your email address below to be notified when it becomes available again		

A covert calculator for all your corporate espionage needs, only £199.00!! (VAT not included) [\[source\]](#)



GSM PIR Sensor Bug

This GSM PIR is a cleverly disguised hand-made listening device (GSM bug) that has been manufactured for totally discreet room monitoring. A unique movement sensor makes this GSM Audio Bug stand out from the crowd.

Shipping in 24 hours
Product out of stock

[Ask A Question](#)
[Product Shipping](#)

Product Code GSM3	£ 199.00 ex. VAT	£ 238.80 inc. VAT
This product is currently out of stock, please fill in your email address below to be notified when it becomes available again		

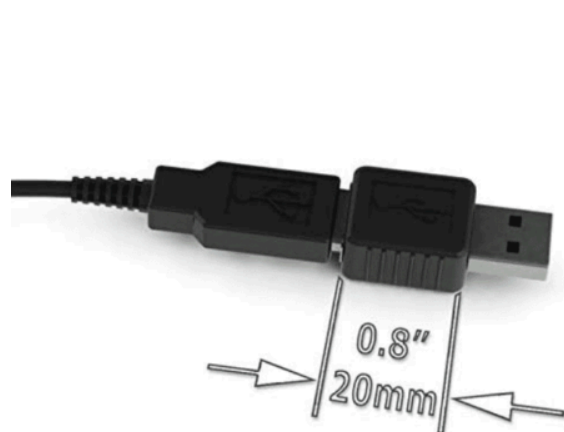
A bugging device disguised as a security sensor. When the sensor is activated the device begins recording conversations in the room. [\[source\]](#)

3.2 Intercepting Computer Data

The vast majority of corporate espionage cases involve stealing data from computers. Certainly, in the modern age, computers are the primary means of storing and disseminating information. Two means can extract computer data – through hardware or software. The former involves planting a device within a system, whereas the latter is through remote means, like malicious software or hacking.

3.2.1 Hardware

Keyloggers or key capturers are small hardware devices that record keystrokes. By plugging the device into a keyboard or laptop, a snooper has access to vital inputs such as passwords.



KeyGrabber Pico USB 8GB - Tiny Hardware USB
Keylogger with 8 Gigabyte Flash Drive
Brand: KeyGrabber
5.0 ★★★★★ 1 rating

€41⁹⁹

Brand	KeyGrabber
Memory storage capacity	8 GB
Hardware interface	USB
Special feature	Lightweight
Connectivity technology	USB

About this item

- Lightweight

A key logger available online measuring at less than an inch. [\[source\]](#)

Further mediums include USB drives and mobile phones which are capable of high quality imaging and audio recording, and which can be easily shared through encrypted messaging apps. Information can also be leached via network services such as emails and virtual private networks (VPN). [\[source\]](#)

3.2.2 Corporate espionage software

Software based espionage has the benefit that it can be conducted remotely and the target can be surveilled over a longer period of time. A few examples of malicious software include Spyware, Scareware, Ransomware, Adware, Trojan Horses and Viruses. All either blackmail the target into handing over sensitive information or take remote control to directly extract said information. [\[source\]](#)

Corporations rely on wireless communication networks to transmit information which are vulnerable to interception. By intercepting wireless communication, the attacker can launch Man-in-the-middle attacks. [\[source\]](#) As the “man in the middle” the attacker can eavesdrop on conversations, alter messages or cause DoS (Denial of Service) attacks. Typically, the attacker achieves the attack by setting up an interception communication station and then tricking the target’s communication provider into believing that the interception station is genuine. [\[source\]](#)

4. Corporate espionage case studies

4.1 Uber Uses Spyware to Crush Rival – 2024

In April 2024, an Australian court alleged Uber used corporate espionage to undermine car-sharing rival GoCatch. [\[source\]](#) The court heard that Uber used a scraping software called “surfcam” on GoCatch driver’s phones to collect information. The spyware was modified and developed in-house at Uber’s HQ in Sydney. GoCatch claims that the information collected since 2012 has unfairly stolen market share, putting Uber in a market-leading position across Australia. [\[source\]](#)

4.2 Selling Coca-Cola’s Secret Formula to Pepsi – 2006

In 2006, Joya Williamson, the administrative assistant to the Global Head of Marketing at Coca-Cola attempted to sell Coca-Cola’s secret recipe to market rival PepsiCo. [\[source\]](#) Disgruntled with her role at Coca-Cola, Williamson stole a phial of an unreleased Coca-Cola product and attempted to sell it to Pepsi for \$1.5 million (£800,000). Unwilling to restart the Cola Wars, Pepsi suspected the phial to be stolen and alerted Coca Cola as well as the FBI. In response, the FBI set up a sting operation to catch Williamson and her accomplices. In May 2006, an FBI agent posed as a man called “Jerry” and

claimed to be a Pepsi executive. “Jerry” exchanged Coca-Cola’s secret formula for \$30,000 cash stuffed in a child’s lunchbox. [\[source\]](#)

Joya Williamson and her accomplices Ibrahim Dimson and Edmund Duhaney had been caught red handed. Charged with wire fraud and unlawfully stealing and selling trade secrets, Williamson was handed eight years in prison, with Dimson and Duhaney receiving two and five years respectively.

4.3 The Third Party Threat at Gillette – 1997

Not all corporate espionage threats come from within. In 1997, Steven Louis Davis, a subcontractor for Gillette, stole and shared trade secrets worth \$750 million. These trade secrets were a new shaving system Gillette had yet to release. Davis was working for Wright Industries, a third party design company. In 1997, Davis became disgruntled with his working condition and feared his job was at stake. As a Gillette subcontractor, Davis had access to proprietary information. Davis decided to email and fax information on Gillette’s upcoming shaving products to industry competitors. Gillette reported Davis to the FBI. The plea deal significantly reduced Davis’ sentence from 15 years in prison and a \$250,000 fine to just 2 years.. [\[source\]](#)

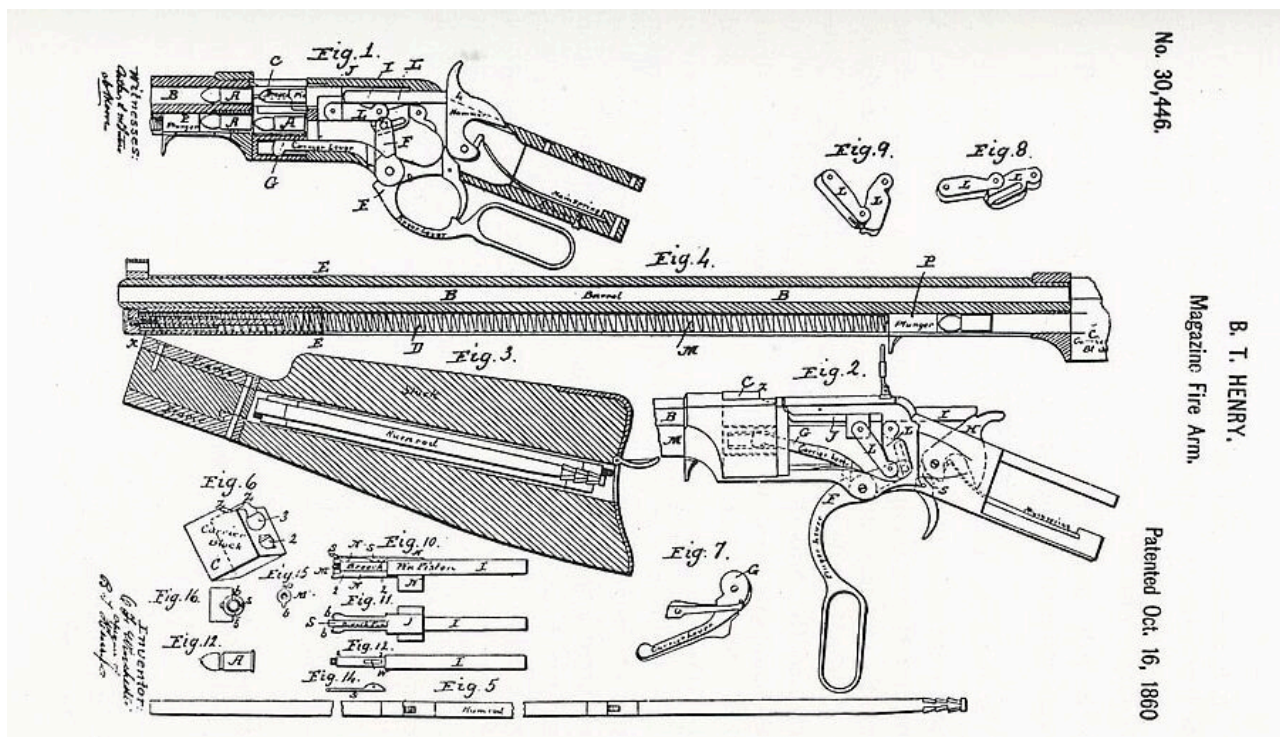
5.0 How do you counter corporate espionage?

Innovation is the lifeblood of the business world. Corporations that are unable to innovate or protect their innovations lose their competitive advantage and consequently their market share. It is therefore imperative that businesses invest in countermeasures to mitigate the risk of corporate espionage and intellectual property theft. As explored in previous examples, information breaches can cost corporations hundreds of millions of dollars and untold damage to their brand and reputation. This section will explore the technical and non-technical means of countering corporate espionage.

5.1 Legal protection

Patents are arguably the strongest protection corporations have against espionage and theft. Patents grant companies exclusive rights to produce and sell their innovations. Furthermore, they establish a legal framework that enables companies to sue competitors who imitate patented designs. While this provides protection within the corporation’s national borders, enforcing patents internationally is significantly more challenging.

For example, throughout the twentieth and twenty-first century Chinese companies have consistently stolen American intellectual property. According to a 2019 US government paper, not only have Chinese authorities done little to prevent IP theft, they have actively incentivised the stealing of foreign technology. [\[source\]](#) US companies are unable to rely on the patent system to internationally protect their innovations from theft. Therefore companies must look beyond legal countermeasures and take responsibility for IP protection themselves. This is where in-office countermeasures in the next section come in.



5.2 Security Awareness Training

5. Equipment



This is a hand-held frequency receiver. [[source](#)]

A frequency receiver is essentially a high-quality walkie-talkie. Being highly sensitive and equipped with excellent frequency resolution, the device can differentiate between signals that are close in frequency. This enables the device to detect hidden cameras or other wireless devices planted for eavesdropping. [[source](#)]



Larger desktop frequency scanners. Modern frequency scanners can be connected to PCs. [source]

5.2.2 Detecting Devices Without a Signal

The second kind of device is Non-Linear Junction Detectors (NLJD). This device detects components rather than signals. This device enables the detection of eavesdropping devices that do not emit a signal. NLJDs detect components such as diodes, transistors or integrated circuits.[source]



Resembling metal detectors, Non-Linear Junction Detectors are capable of detecting eavesdropping devices that do not emit signals, are not powered or have even ceased to

operate. [\[source\]](#)

5.2.3 Detecting Other Eavesdropping Devices

Infrared cameras can also spot hidden cameras. When infrared light shines on a camera lens, it creates an intense reflection identifiable by a lens detection device. This system does have the drawback that other items, such as screens and mirrors, will generate a similar reflective signal.

With regards to detecting telecommunication interception, systems once again range for simple plug-in devices to sophisticated analysers. All telecommunication interception countermeasures rely on the same principle of monitoring phone lines for variations in voltage. If the monitoring system detects an increase in voltage during a phone call, it likely indicates that someone has tapped the phone line.

6. Conclusion

Corporate espionage remains a pervasive threat in today's interconnected business landscape. As companies strive to maintain their competitive edge, the temptation to resort to unethical means can be strong. However, the consequences of engaging in such activities are severe, not only in terms of legal repercussions but also in damaging trust and reputation to a corporation. Therefore, it is imperative for a corporation to invest in robust security measures to safeguard their intellectual property.

The future of corporate espionage appears poised for further complexity and innovation. With advancements in technology and the proliferation of interconnected systems, the avenues for clandestine intelligence gathering are bound to expand. As with all forms of intelligence collection however, countermeasures to corporate espionage are likely to remain on the backfoot, perpetually playing catch up with the latest technological innovation.