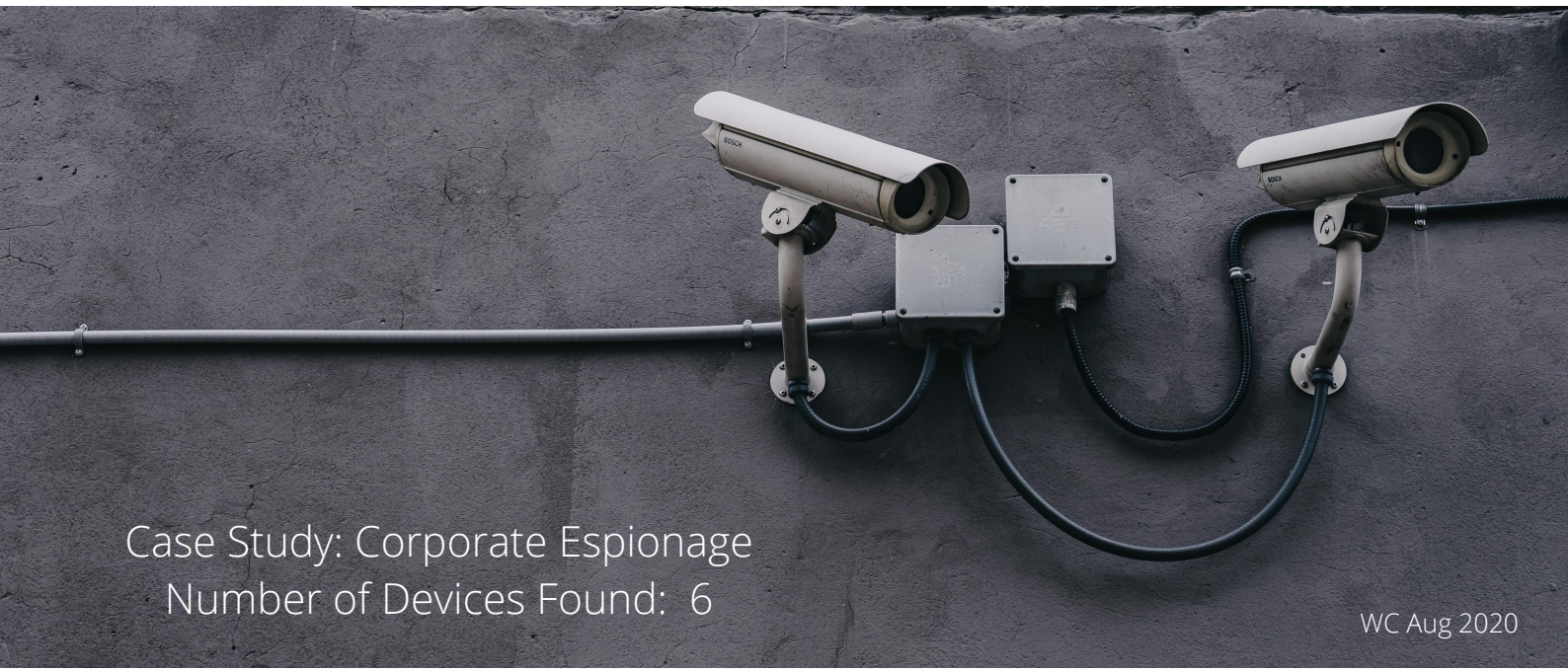
Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

2020: THE "BUGGING" WARS MARCHES ON

"And you thought spy stories were a thing of the past"



A View Into Modern-Day Corporate Espionage

In this edition we look at how the abuse of authority and technology can be used to infiltrate and spy on trusted sources within an organisation.

What started off as a routine installation and upgrade to the Closed-Circuit Television (CCTV) infrastructure, soon turned into a project that was tainted by the installation of covert cameras - used for malicious eavesdropping purposes against senior members of management of the organisation.

These types of threats are real and imminent, and these scenarios are no longer something that only happens in Hollywood blockbusters.

The events leading up the TSCM / "Debugging" investigation

A Gauteng based manufacturing company initiated a project to upgrade their existing CCTV infrastructure during 2019. The project was entrusted to a works manager, also a full-time employee of the company, to manage and ensure that the project was delivered in line with the security requirements set forth by management.

The vendor selection process was completed, and the preferred vendor was selected to supply the required CCTV equipment for the project. Phase 1 of the project focused on the installation of 10 surveillance cameras to monitor and prevent copper theft that had plagued the company. Phase 1 was completed, and preparations were made to initiate Phase 2 of the project. It was at this stage where the project was steered into murky water by the works manager.

The works manager requested that covert cameras be installed at strategic pinpoints throughout the premises. He instructed the vendor to not list these cameras as covert or spy cameras on the invoice, as this would raise suspicion with the finance department. The motives of the works manager was never questioned, as he was a trusted employee to the company, and the project lead on the project. Phase 2 was completed, the invoice details changed to not raise suspicion, and the vendor invoices were processed without any questions being asked.

Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre
INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

The cry for help and how we assisted with a TSCM / "Debugging" investigation

During 2019, the CEO of the company, stumbled upon, and discovered one of the covert cameras by accident. The CEO immediately raised the alarm, and contacted Advanced Corporate Solutions (ACS), specialist in the field of Technical Surveillance Countermeasures (TSCM / "Debugging") to assist with a formal investigation into the matter.

The team from ACS arrived on the scene, and initiated a detailed sweep of the offices and areas of concern. Making us of sophisticated, state of the art equipment, the team discovered any companies worst nightmare - covert cameras, that were strategically and maliciously installed for eavesdropping purposes. A total of 6 devices were discovered during the sweep. The devices were installed and concealed in the elevator, office of the CEO, main boardroom, reception area, ICT offices and finance offices.

The CEO requested further assistance and investigation into the matter. which in turn instituted a formal forensic investigation led by ACS and Dynamdre. The digital forensic investigation was conducted in accordance to industry best practices, which included the acquisition, imaging and forensic analysis of all devices uncovered during the sweep.

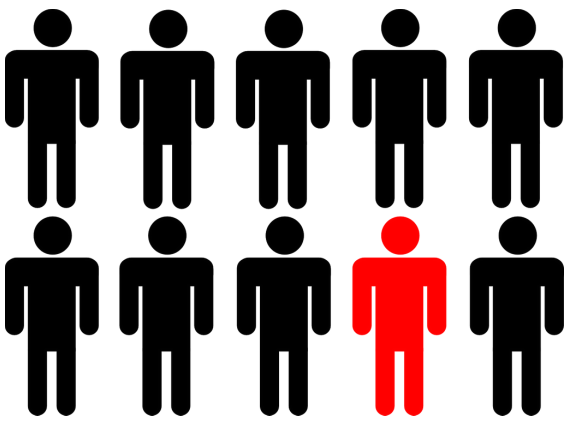
Lets take a look at the devices that were discovered

A - Camera
B - Arial to Connect to WiFi
C - Battery Pack
D - Main Device

The devices had the capability to record both video and audio within the areas they were installed . The recordings could either be stored locally on the device by utilizing the on-board SD Card, or could be streamed to any remote location via the software application. The devices were connected the WiFi and internet infrastructure, which gave the perpetrator access to the devices and recordings, without even being in the office environment.

Tho make matters worse that the perpetrator could have audio-visual access to confidential conversations, presentations and information assets shared within the areas in which the devices were installed.

This certainly gives new meaning to the term "INSIDER THREAT"



What can we learn from this?

"A chain is only as strong as its weakest link." The same is true for information security, where corporate espionage and information leakage are often the result of employee actions. We need to create and implement formal awareness programs to educate our employees on the threats and attacks on intellectual property they unknowingly face on a daily basis.

We need to re-evaluate our levels of trust within our organisations. An insider threat is a security risk that originates within the targeted organisation. This doesn't mean that the actor must be a current employee or officer in the organisation. They could be a consultant, former employee, business partner, or board member. We need to implement formal processes that governs, monitors and manages employees and contractors; this includes screening and vetting process as well as segregation of duties.

We cannot emphasize the importance of continuous assessments, with a focus on continuous improvement of information security vulnerabilities uncovered during these assessments. The focus of your assessment strategy should be on the safeguarding of intellectual property and information assets in accordance to:

Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

What can you do?

Your information security assessment strategy, should at the very least, include the following key elements:

1. TSCM / "Debugging" Sweeps / Assessments - Skilled TSCM / "Debugging" assessments needs to be conducted on a regular basis, at least once a month in high-profile areas of your organisation.
2. Penetration Testing and Vulnerability Assessments - Skilled penetration testing at least twice a year, and vulnerability assessments preferably every second month.
3. Remediation Planning and Reporting - Vulnerabilities, uncovered during these assessments, should be classified in accordance to their severity, and fixed accordingly. Progress on remediation should be monitored and reported on, on a monthly basis to senior management.
4. If you are unsure, or need guidance, contact the specialists - our expertise are but a phone call away. Contact us today and find out how we can assist you in improving your information security posture, and safeguard your intellectual property.

Advanced Corporate Solutions
TSCM | "Debugging" Specialists | Service Excellence since 1995

dynamdre INNOVATIVE SOLUTIONS
Information Security I www.dynamdre.co.za

Riaan Bellingan (Snr)
Office: +27 (0) 12 349 1779
Cell: +27 (0) 82 491 5086
Email: riaan@acsolutions.co.za
Website: www.acsolutions.co.za

Riaan Bellingan (Jnr)
Office: +27 (0)12 880 2238
Cell: +27 (0) 72 671 5764
Email: riaan@dynamdre.co.za
Website: www.dynamdre.co.za