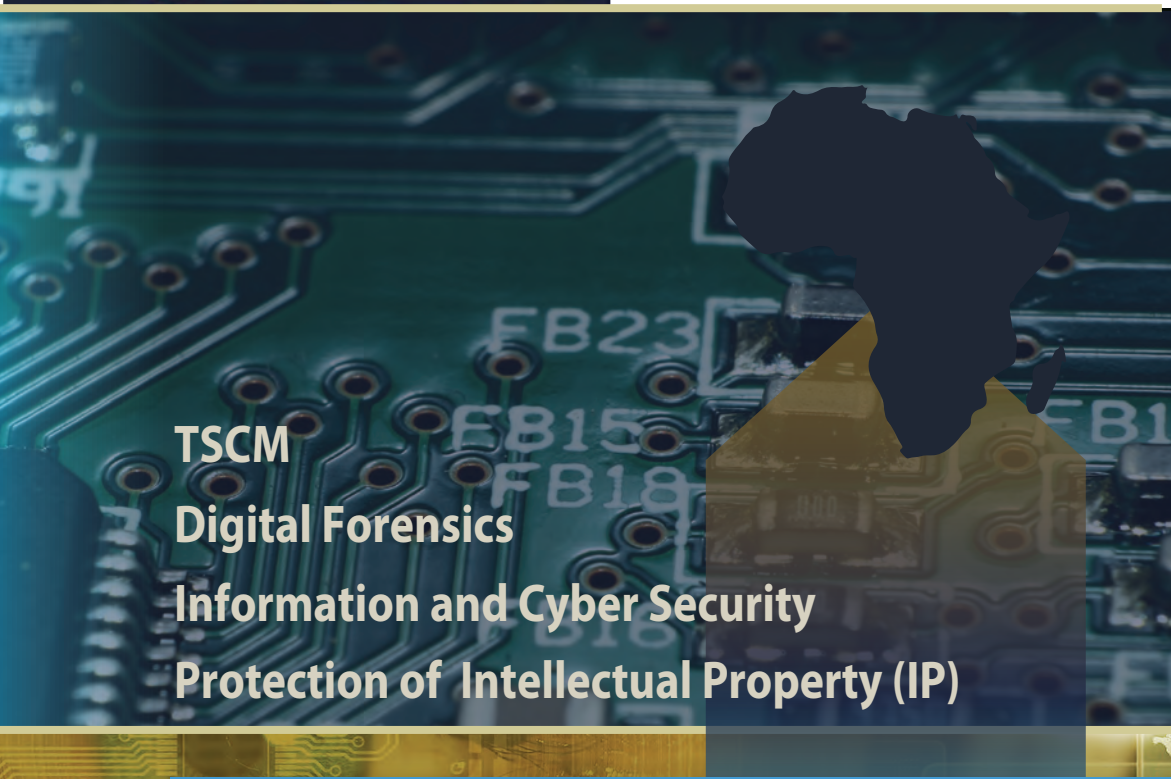
Advanced Corporate Solutions
"Debugging" Specialists | Service Excellence since 1995

dynamdre
INNOVATIVE SOLUTIONS



TSCM
Digital Forensics
Information and Cyber Security
Protection of Intellectual Property (IP)

SERVICE OFFERINGS
BY ACS/DYNAMDRE

We pride ourselves on well-established accreditation and association with the following local and international authorities and bodies:

South African Police Service
Reg. No. : 4000271

Private Security Industry Regulatory Authority
Reg. No.: 0958804

Safety and Security Sector Education and Training Authority
Reg. No.: 051901409857

Association of Certified Fraud Examiners
SA Chapter

REI USA

SHEARWATER

Blake Technical SARL

Espionage Research Institute International

TABLE OF CONTENTS

Technical Surveillance Counter Measures (TSCM)

Corporate eavesdropping poses a significant risk to organisations. Global statistics demonstrate that the threat of internal eavesdropping is real, imminent and ongoing. The majority of eavesdropping devices found during "Bug Sweeps" are planted either by current employees, IT personnel and recently terminated employees or associates.

Intellectual Property (IP) and Information Assets, including, but not limited to, trade secrets, product design, development or pricing and other proprietary information, are critical to any business remaining functional and competitive. Yet this data is routinely exposed to the risk of theft and is overlooked in Information and Cyber Security Risk Management, and organisations are increasingly ineffective at safeguarding such information.

As breach notification laws, regulatory requirements, and reputational considerations draw increasing focus to Information and Cyber Security, regarding the personal data of clients, customers or personnel, businesses are risking their most valuable assets, and that risk has a notable price tag.

For many businesses, IP protects more than just an idea or a concept – it protects genuine business assets that may be integral to the core services of its operations and their overall long-term viability.

IP can consist of various aspects, ranging from corporate identity through to products, services and processes that differentiate a business' offering. When an organisation's concepts, processes and ideas are used without permission, it is prejudiced.

Almost all businesses have undoubtedly benefited from the Internet, where products, services and marketing communications can reach vast audiences at relatively low cost, but this has also increased the chances and instances of Intellectual Property theft.

Companies, irrespective of size or jurisdiction, are at increasing risk of having their unique ideas, products or services infringed upon, making IP protection more important than ever.

The equipment utilised by ACS/Dynamdre is manufactured by leading producers based in the United Kingdom and the United States of America and follows stringent maintenance schedules, ensuring operating capacity and the highest levels of accuracy. The equipment listed below is used to conduct a physical search that covers areas commonly used to conceal eavesdropping devices etc.

Set out below is an overview of equipment options utilized by ACS/Dynamdre during TSCM assessments and inspections.

OSCOR™ Blue Spectrum Analyzer

The OSCOR Blue is a portable spectrum analyser with a rapid sweep speed and functionality suited for detecting unknown, illegal, disruptive, and anomalous rogue transmissions across a wide frequency range. The OSCOR Blue Spectrum Analyzer is designed to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum.

MESA – Mobility Enhanced Spectrum Analyser

The MESA is a portable, handheld RF receiver that detects known, unknown, illegal, disruptive, or interfering transmissions. The MESA features unsurpassed mobility and ground breaking features, not found in any other spectrum analyser. First in its class, the MESA is purpose built to locate unknown signals throughout a wide frequency range up to 6 GHz. DETECTS: RF Wi-Fi, Bluetooth, Cell phones and Illicit transmissions (Eavesdropping "Bug" Detection).

Kestrel TSCM® Professional Software

Kestrel is a highly evolved TSCM specific, operator centric SDR application, with advanced capability to meet TSCM specific and evolving challenges of professional technical operators, working in the private sector, and within the national security apparatus, who are faced with a modern moving target threat model, in combating the growing threats of cyber-espionage. The Kestrel TSCM® is not a simplistic desktop spectrum analyzer, offering limited capability, but rather, it is a highly deployable, mission scalable, travel friendly full featured TSCM focused product.

Raptor RXi

The Raptor RXi is an ultra-fast-scanning counter-surveillance receiver, capable of scans from 10 kHz to 26 GHz in under 4 seconds, for quick detection of surveillance transmitters and with the ability to detect even the briefest pulsed transmissions. Featuring a fast Core 2 Duo processor, its multiple software tools and demodulators detect frequency hopping, burst mode and spread spectrum devices as well as analogue audio and video signals.

A.N.D.R.E Deluxe - Advanced Near-Field Detection Receiver

The Advanced Near-Field Detection Receiver (A.N.D.R.E) is a broadband receiver that detects nearby ambient Radio Frequency (RF) energy. It provides an economical tool for detecting known, unknown, illegal or disruptive, or interfering RF transmissions across a 10 kHz to 6 GHz frequency range.

CPM-700

The CPM-700 is a broadband receiver designed to detect and locate all major types of electronic surveillance devices, including (but not limited to) room, phone, body bugs, video transmitters, and tape recorders. Such broadband receivers provide a very important cost-effective tool for professional sweep teams, government security personnel, and private citizens with important security needs.

TALAN™ 3.0 Telephone & Line Analyser

Voice-over Internet Protocol (VoIP) phone systems present a new form of security risk to an organisation's communications. With new enhancements built into the TALAN software interface, users can now test Internet Protocol (IP) packet traffic on VoIP phones and systems. VoIP data collected by the TALAN software includes source and destination Mac addresses, header type, statistics (including total packets, packet rate, peak rate, and run time). Users can also define advanced filtering options. Data can be stored and exported to USB or flash drive as data files for further analysis, sharing and reporting.

HAWK XTS-2500

The HAWK XTS-2500 is a portable, accessible advanced electronic device detector, also known as a Non-Linear Junction Detector (NLJD). The HAWK XTS-2500 is capable of locating and confirming the presence of electronic components found in devices, regardless of whether they are switched on or off.

Bloodhound

Bloodhound is an Acoustically Stimulated Microphone Detector (ASMD), which is an electronic system for use by Technical Security Inspection Teams for detecting audio eavesdropping devices. The system works by detecting the radiated field created whenever a microphone detects sound. The Bloodhound operator can either listen to the detected audio or establish acoustic feedback.

Video Pole Camera

The Video Pole Camera provides white LED illumination for colour inspection in dark areas, i.e. drop ceilings, behind immovable objects, around corners, and other difficult to reach areas and in dark situations.

Seek ShotPRO Thermal Imaging Camera

The Seek ShotPRO is the most advanced thermal imaging camera for professionals. Photos and videos are analysed immediately with new on-board thermography tools. Spot measurements and temperature boxes are created for time-saving reports. Problems are precisely diagnosed with 16 x higher resolution.

CAT/ FLIR Camera and FLIR One

Powered by FLIR's Lepton® camera and using FLIR's exclusive MSX® technology. This rugged device uses FLIR (Forward Looking Infrared) to capture clear thermal imagery, video and even time-lapse footage. The thermal imaging technology is used in the field of TSCM to determine if there are any hidden or rogue electronic devices in the vicinity. Electronic devices have multiple ways of accessing power sources on order to function, which inevitably leads to the emission of heat. The device is also used to identify and locate rogue Wi-Fi access point in a target area.

DIGITAL FORENSIC SERVICES

As smartphones and tablets become constant companions, hackers are seeking every avenue available to break into them.

Many people expect that iPhone or Android devices are secure by default, when in reality, it is up to the user to make enhanced security configuration changes. With the right (inexpensive) equipment, hackers can gain access to a nearby mobile device in less than 30 seconds and either mirror the device and see everything on it or install malware that will enable them to siphon data from it at their leisure.

The nature and types of cyber-attacks are evolving rapidly and, with good reason, mobile devices have become a critical part of enterprise Cyber Security efforts. Research firm, Gartner, predicts that by 2021, 27% of corporate data traffic will bypass perimeter security and flow directly from mobile and portable devices to the cloud.

Mobile malware threats are typically socially engineered and focus on tricking the user into accepting what the hacker is selling. The most prolific include spam, weaponized links on social networking sites and rogue applications. While mobile users are not yet subject to the same "Drive-By" downloads that PC users face, mobile advertisements are increasingly being used as part of many attacks, a concept known as "malvertising".

Android devices are the biggest targets, as they are widely used and easy to develop software for. Mobile malware Trojans designed to steal data can operate over either the mobile phone network or any connected Wi-Fi network. They are often sent via SMS (text message); once the user clicks on a link in the message, the Trojan is delivered by way of an application, where it is then free to spread to other devices. When these applications transmit their information over mobile phone networks, they present a large information gap that is difficult to overcome in a corporate environment.

Cellebrite is a world leader in the development of advance mobile forensic hardware and software products. The Universal Forensic Extraction Device (UFED) Touch Ultimate from Cellebrite is an example of hardware used by mobile device investigators to gather information from mobile devices that may contain infected and malicious data.

INFORMATION AND CYBER SECURITY SERVICES

Information and Cyber Security consists of the collection of technologies, standards, policies and management practices that are implemented to guarantee that information remains secure. Information Security policies and tools assist an organisation in preventing, detecting and countering any threats to information, whether the information is digital or non-digital. Information is a major asset in any company and as such must be handled with due care.

Why is it important to secure company information?

Information and Cyber Security prevents company information from making its way into the hands of parties who are not authorised to have access to such information, and who may use the information for malicious purposes.

Ensuring that a company's information is secure is essential, considering that the leakage of confidential information could potentially be detrimental to the operations of any business.

Corporate Governance, on the other hand, refers to the structures and processes for the direction and control of companies. Corporate Governance also concerns the relationships between management, the Board of Directors, controlling shareholders, minority shareholders and other stakeholders. (Refer to King IV Report: SA)

Effective Corporate Governance helps companies operate more efficiently, improves access to capital, assists in mitigating risk, and safeguards against mismanagement. It makes companies more accountable and transparent to investors and gives them the tools to respond to legitimate stakeholder concerns such as sustainability, operational, environmental and social issues. Information Security, though often viewed as a set of technical issues, must be embraced as a Corporate Governance responsibility that involves risk management, reporting controls, testing, training and executive accountability.

Our methodology is built on three important pillars that are vital to the success of these types of projects and your business:

Confidentiality: Data is only accessed by those with the right to view the data.

Integrity: Data can be relied upon to be accurate and processed correctly.

Availability: Data can be accessed when needed. Failure to comply with the requirements of Information Security Guidelines may lead to disciplinary action.

Our assessment methodology consists of the following approaches:

A Security Assessment is conducted to determine:

- The degree to which Information System security controls are correctly implemented;
- Whether they are operating as intended; and
- Whether they are producing the desired level of security;

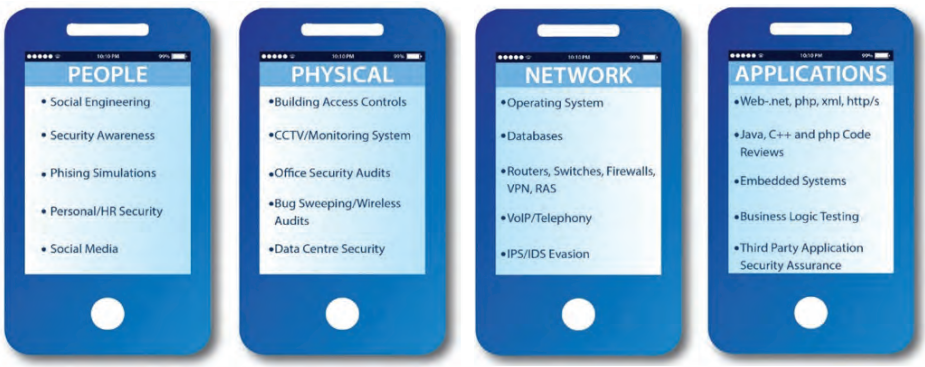
A Vulnerability Assessment is conducted to determine:

- Inherent weaknesses in the Information Systems that could be exploited, leading to Information Systems breaches; and

Penetration Testing (Pen-Test) is conducted to:

- Evaluate the security of an organisation's Information Technology (IT) infrastructure by trying to exploit vulnerabilities under controlled conditions, including any that may be present in operating systems, service and application flaws, improper configurations, or risky end-user behaviour.

The areas of evaluation cover the following specific aspects:



INFORMATION AND CYBER SECURITY AWARENESS

One of the greatest threats to Information Security could come from within an organisation itself, with a possible spectrum ranging from disgruntled workers and corporate spies to the non-malicious, uninformed employee. "Inside attacks" have been noted to be some of the most dangerous since these people are already reasonably familiar with the infrastructure and have cause to be present and engaged within a business.

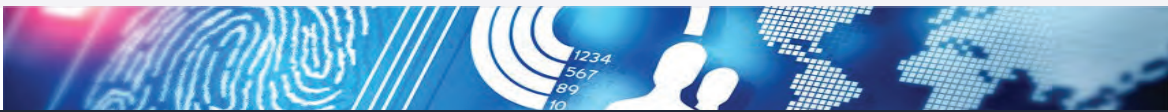
ACS/Dynamdre's focus is on uninformed users who can do harm to an organisation's network by visiting websites infected with malware, responding to phishing e-mails, storing their login information in an unsecured location, or even giving out sensitive information over the phone when exposed to Social Media engineering.

One of the best ways to make sure company employees will not make costly errors with respect to Information Security, is to institute company-wide security awareness training initiatives that include, but are not limited to, the conduct of classroom style training sessions, access to security awareness websites, regular provision of helpful hints via e-mail, or even awareness posters placed prominently within a company's offices.

These methods can help to ensure employees have a solid understanding of company security policy, procedure and best practices and that their critical nature and consequences of a breach are constantly affirmed.

ACS/Dynamdre's information security awareness program covers the following key daily risks:

- **Introduction to Cyber Security**
- **Mobile Devices**
- **Passwords**
- **Data Protection**
- **Insider Threat**
- **Malware**
- **Ransomware**
- **Phishing / Advanced Spear Phishing**
- **Physical Security**
- **Security Outside the Office**
- **Business Email Compromise**
- **Social Engineering**
- **Malicious Links**
- **Social Networking**
- **Surfing the Web**



PROTECTION OF INTELLECTUAL PROPERTY (IP)

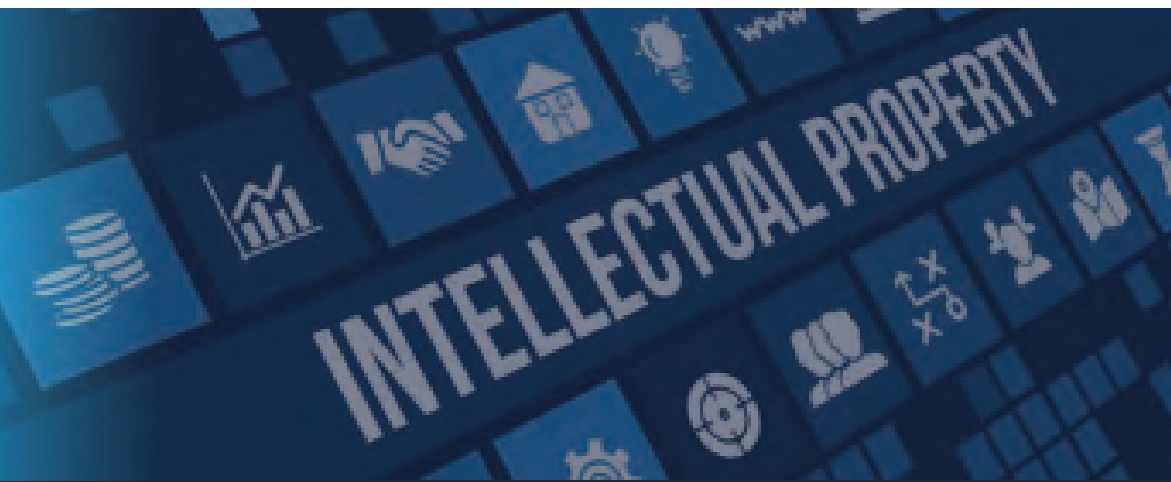
1. Introduction: What is Intellectual Property (IP)?

Intellectual property normally refers to creations of the mind, inventions, artistic works, symbols, names, designs etc. It is being described as property because it can be owned, sold or transferred. Intellectual property may include the following: patents, trademarks, registered designs, breeder's rights, copyrights or circuit layout rights.

The International Commercial community regards trade secrets as the intellectual property of a specific business or company. Per definition trade secrets are protected information which is not generally known amongst or readily accessible to persons and has commercial value because it is secret. Trade secrets are normally not protected by law as are patent rights and therefore trade secrets have to be protected by the company/institution/corporation itself.

The following business interests would inter alia be regarded as trade secrets and need to be protected:

- Board of Directors' and confidential meetings
- All strategic planning and operations, financial, marketing, sales strategies etc.
- Financial affairs, including annual returns up to period of publication
- Investor Relationship
- Acquisitions and mergers
- Information that could affect a company's share price, if a listed company.
- Patent rights
- All confidential information that would benefit a competitor or give a competitor an advantage over your own company.
- Existing security procedures and modus operandi to protect trade secrets



2. Areas of communication vulnerability that could lead to breach of trade secrets:

COMMUNICATION SECURITY: VERBAL

- Offices
- Boardrooms
- Premises of VIPs of business or decision makers
- Residences of VIPs of business or decision makers
- Vehicles of VIPs of business or decision makers
- Offices of Service Providers which deal with secret information

COMMUNICATION SECURITY: TELEPHONE OR MOBILE

- Analogue Systems
- Digital Systems
- Voice over Internet Protocol (VoIP) Telephones and Systems

INFORMATION TECHNOLOGY: GATEWAYS

- One or more Central Processing Units (CPU)
- Operating System
- Network Interface
- Disk Drives
- Embedded Web Server
- PDL Interpreter Postscript
- Local User Interface
- Local Hardware Ports
- Fax System
- VoIP System

DOCUMENT SECURITY

- No Policy on document management
- Outsourcing of printing of classified documents
- Internal printing of classified documents
- Disposal of classified documents
- Record keeping of classified documents

DIRECTORS, EXECUTIVES AND PERSONNEL

- No HR policy on integrity assessments
- No regular integrity assessments on key personnel and directors
- No regular integrity assessments on Service Providers dealing with confidential or sensitive matters

PHYSICAL SECURITY

- No regular surveys on locks, doors, windows, access and control

3. Threat to communication security

Although the technological advancement in all spheres of life is affecting every human being on the planet, either positively or negatively, it is a reality that technology has also brought new challenges to commercial enterprises. For the purposes of this discussion we will only focus on communication and the challenges it poses.

It is important to realize that there are no secrets anymore if technology is utilized and it is becoming easier every day to access information on every level, from open to top secret.

There are still some companies and corporate institutions, even listed companies that live in a state of denial. "We have nothing to hide or who would want to infiltrate us and for what reason."

We must realize that in White Collar Crime, in respect of communication theft is a big business and very, very profitable. Due to the fact that it is embarrassing for companies to fall prey to communication penetration, it is very seldom reported in the media. Commercial espionage is currently at its highest peak ever. The economic competition amongst major powers and conglomerates is rife and no money is being regarded as wasted, as long as the information has a price tag.

The biggest targets today around the world are so-called blue chip listed companies, with specific emphasis on the decisions and financial affairs of these companies.

4. Mobile devices

Mobile devices, which include smart phones and tablet computers, provide increased functionality and ease of use to people, anywhere and anytime. Smart phones are the new computers. These devices contain a tremendous amount of personal and business information. With rapidly increasing advances in technology, everyday life is starting to depend on these wireless devices, which unfortunately also exposes the user to greater risk and some unique security threats.

Mobile device malware (malicious code) has increased exponentially over the past few years. The sophistication of these exploits has also increased exponentially, making detection and eradication very difficult. Anyone can install eavesdropping software on your smart phone, as long as they have access to your phone even for a few minutes. This can result in them gaining access to all your private data such as; SMS, emails, pictures, location information, call logs and even listen in on actual calls. Some malicious codes will even allow the attacker to switch on the microphone of the device unnoticed and listen in on conversations or use the camera to secretly take a picture.

Cellebrite is a world leader in the development of advanced mobile forensic hardware and software products. The Universal Forensic Extraction Device (UFED) Touch Ultimate from Cellebrite is an example of hardware used by mobile device investigators to gather information from mobile devices which may contain infected and malicious data. Note that on request, we can assist and conduct an TSCM Threat Analysis on a mobile phone.

5. Solutions

The first step is to realize that there is a real threat and all forms of communication needs to be protected. It is important to obtain the services of a specialist in the field of communication to analyze the existing policy, procedures and protecting of communication. To achieve this goal the specialist needs to execute a vulnerability assessment on all forms of communication. This would include the following:

- TSCM - Offices, Boardrooms, Premises etc.
- TSCM - Residential Premises and corporate vehicles of Key Personnel
- Mobile Devices tested for Spyware
- Telephone Line Testing: Analogue, Digital and VoIP
- Pen testing in respect of VoIP
- Survey on Document Security, Policy and Procedures
- Survey on Physical Security that could affect communication security
- Detail report on vulnerability assessment
- Policy on communication security
- Monitor and audit
- Secure Management

CONTACT US

Contact the following ACS/Dynamdre executives to arrange a full briefing on these options to ensure your organisation's compliance and best practice in this critical area of Information Security:

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

Dynamdre
Riaan Bellingan (Jnr)
Office: +27 (0) 12 349 1779
Cell: +27 (0) 72 671 5764
Email: riaan@dynamdre.co.za

First Floor, Building 16, CSIR, 627 Meiring Naude Road, Brummeria, Pretoria, Gauteng, South Africa, Gate 3, 525 44.874, E028 16.523