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

dynamdre
INNOVATIVE SOLUTIONS

PROTECTION OF INTELLECTUAL PROPERTY (IP)

INTRODUCTION
TO 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

ABOUT ADVANCED CORPORATE SOLUTIONS (ACS)

Advanced Corporate Solutions is a well-established business which was founded in 1995 and since then served their clients with pride and dignity.

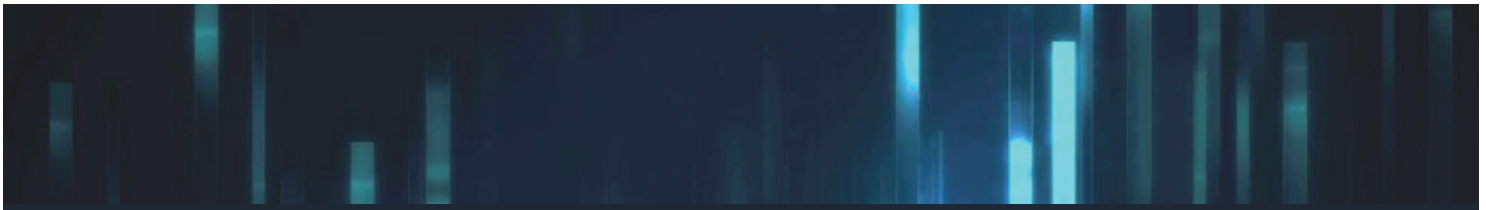
The business, with its primary focus on Protection of Intellectual Property (IP), therefore Technical Surveillance Countermeasures (TSCM) "Debugging", has over the past twenty three years proved themselves as a leading business in these fields. What clearly distinguishes Advanced Corporate Solutions from their peers in South Africa, is that they developed an international network of associates that not only keep themselves abreast of international trends, but also enhance their training of personnel and quality of equipment to meet international standards and benchmarks.

Advanced Corporate Solutions (ACS) and Dynamdre specialises in current best practice interventions and solutions for the identification and management of Information Security. This brochure sets out the options and the case for urgent intervention and ongoing management by ACS/Dynamdre.

If there was a current weakness in your organisation's Information Security profile, would you not want to know about or find it before someone with malicious intent does?

Imagine waking up tomorrow morning to find that your Information Systems have been "bugged", "hacked" or compromised, which may include consequences such as leaking of your organisation's financial results, sale of your trade secrets to your competitors, or publication of your client's information on the internet. Consequences may include loss of confidence in your abilities by your clients; your share price could take a huge plunge; your Board of Directors would be held responsible for inadequate risk management practices. Sound scary? It is. An extreme example? Perhaps. An increasingly prevalent threat? Undoubtedly.

This is because the global operating environment is highly interconnected, ever more technical and interdependent and in real time, with no room for error. The fact is that every single organisation is presently and increasingly dependent on its Information and Information Assets, which are vitally important for the success and future existence of a client's organisation, and which need to be protected accordingly. This is irrespective of whether an organisation is located in Africa, the United States of America, Europe or South-East Asia – each threat holds the same levels of urgency and severity of consequences.



So, no matter the size of an organisation, ensuring security of information (Information Security) is of paramount importance for both your own and clients' data. The careful planning and implementation of strict controls which are best practice and bespoke, where necessary.

Following this, ongoing monitoring and maintenance, are imperative to protect a company's assets, especially information, which is extremely valuable to any organisation. Information can be leaked by utilizing eavesdropping devices (bugs), mobile devices (malware/spyware) or hacking of IT Systems. Even a small-scale Information Security breach could leave your business without access to its critical Information and Communications Technology (ICT) systems for hours and even possibly days, impairing operational capability, risk to reputation and value.

Information Security is not only an ICT problem, it is a business issue, and more specifically a risk management, compliance and governance requirement, and needs to be managed accordingly.

If an organisation wishes to survive, let alone prosper, it must grasp the importance of Information Security and implement comprehensive, appropriate and current measures and processes to mitigate the increasing threats and damage associated with Information Security breaches.

Advanced Corporate Solutions (ACS) and Dynamdre are experienced practitioners in the field of Technical Surveillance Counter Measures (TSCM) "Debugging," Mobile- and Cyber Forensics, together with the conduct of these interventions for a broad based, worldwide clientele.

The solution to these threats is a professional TSCM, Mobile Forensics and Information and/or Cyber Security intervention.

All members of ACS/Dynamdre's Assessment and Inspection Team are highly qualified in the field of TSCM and have gone through rigorous training and formal security vetting. This awareness and training is the key success factor of ACS/Dynamdre.

Security awareness and training is very important in any organisation. In most cases, there are limited numbers of security professionals in a company and therefore the training of, and creation of awareness by, a company's employees is very important so as to ensure a joint effort and optimal outcome when dealing with matters of IP Protection.

Security awareness training also ensures that employees are fully alive to the consequences of failing to protect an organisation from outside attack, encompassing a spectrum from criminal penalties to large-scale economic damage to a company and the loss of employment.

Employees should be made fully aware of the importance of securing IP and Information Assets, and precisely which systems require protection, the associated security awareness training program should highlight the key ways in which attackers can gain entry to an organisation's operational and executive environment, and the necessary steps to curtail these risks.

ABOUT DYNAMDRE

Dynamdre (Pty) Ltd is an established Digital Forensic and ICT security service provider. We at Dynamdre strive to provide our clients with quick, innovative and affordable ICT solutions. Where our competitors' focus is volume driven, Dynamdre's processes have been developed to enable quality validations of the investigation conducted no matter the size, and that is what differentiates us from the pack. We have an in-depth understanding and knowledge of Digital Forensics, and our resources are aligned to deliver a product that is of the highest value to our clients.

Our mission is to create and maintain long-term professional relationships with our clients through the provision of effective investigation and our commitment in assisting our clients.

"INNOVATIVE ICT SECURITY AND DIGITAL DEFENSE SOLUTIONS FOR YOU AND YOUR COMPANY"

Dynamdre provides the following services:

- Mobile Forensics
- Computer Forensics
- Network Forensics
- Cyber TSCM
- SDI (Storage Devices Imaging)
- VPT (Vulnerability Penetration Testing)
- Data Recovery as well as Electronic discovery

COMPUTER FORENSICS

Computer Forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence to include the legal processes, the integrity of evidence, factual reporting of the information found, and the ability to provide an expert opinion in a court of law or other legal proceedings with regards to the findings.

Dynamdre guarantees proper management of digital forensic acquisitions regardless of the device that we acquire information from, e.g. computers, laptops, tablets, smartphones, storage devices, and so forth. We seize the device and place it in a secure environment to prevent any contamination. After that, we create two forensic duplicates of the data on which we perform all analytics and investigations, and we return the original device to its owner.

We follow the internationally accepted best practice while collecting, examining, analysing and reporting on any digital evidence. We only make use of the most sophisticated software and hardware. Therefore having a reliable and experienced forensics team at your side can help your organization avoid unnecessary and costly employment litigation.

MOBILE FORENSICS

The ability to keep in touch with family, business associates, and to access emails are only a few of the reasons for the increasing importance of mobile phones. Today's technically advanced cell phones are capable of receiving and placing phone calls, storing data, taking pictures, to name just a few of the numerous functions.

When cell phones were first introduced to the public, they were bulky, expensive, and tough to use but as mobile phones developed and became simpler to use, they also became more vulnerable. Cell phones are perfect to stay connected with others and provide the user with a sense of security, but on the downside, our mobile phones are not only just valuable in themselves, but many of them contain valuable and confidential data.

Mobile phones often, if not always, contain a greater amount of valuable data than computers do which make it very tempting for syndicates to steal your personal information without you even noticing. We can perform specified investigations on mobile devices to suit the particular need of our client. We also provide malware and spyware scans to detect any unwanted eavesdropping.

NETWORK FORENSICS

Network Forensics is the capture, recording, storage and analysis of network events to discover the source of security attacks or other problem incidents. The purpose of Network forensics is to record every packet of network traffic to a single searchable repository to examine the traffic in great detail. Collecting a complete record of network activity can be invaluable for addressing technical, operational, and organizational issues.

Network Forensics can uncover the low-level addresses of the communicating systems, which can be used to trace an action or conversation back to a physical device. The entire content of emails, Instant Messaging conversations, web sur ng activities and le transfers can be recovered and reconstructed to reveal the original transaction. Moreover, the protocol data that surrounded each conversation is often treasured.

The following are only some of the uses of Forensics Network:

- Finding proof of a security attack
- Troubleshooting Intermittent Performance Issues
- Monitoring User Activity for Compliance with IT and HR Policies
- Identifying the Source of Data Leaks
- Monitoring Business Transactions
- Troubleshooting VoIP and Video over IP

PENETRATION TESTING

Penetration testing or ethical hacking is the process of evaluating a Penetration testing or ethical hacking is the process of evaluating a company's ICT security and incident response systems to determine if there are any exploitable vulnerabilities which can be used harm to the organisation or its reputation. In short penetration testing is an attempt to gain access to company resources or information without the target taking notice. Penetration testing can thus be described simply as hacking with permission, also known as 'ethical hacking.'

What we offer:

Black Box Testing: The Black Box assessment is simply a penetration test conducted with little to no knowledge of the target. This type of test is considered to be the most realistic as it most accurately simulates a cyber-attack which someone launches from outside the company.

Grey Box Testing: The Grey Box assessment is a form of penetration testing where the hacker receives limited information on the target. This test most accurately simulates an insider attack which could be conducted by someone employed the organization.

White Box Testing: The hacker obtains all the necessary information, therefore, imitating the type of attack the internal company employees would conduct to test the security of the network.

Web Application Testing: We offer this to our clients to ensure the protection of confidential customer information requested by web applications.

VULNERABILITY ASSESSMENT

Due to the growing nature of the Information Security and Cyber Crime threats, Dynamdre focuses on an Information Security Risk and Vulnerability Management approach that delivers results based on indisputable Information Security Risks and Vulnerabilities, and not just on best practice audits. Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. However, why is it important to ensure the security of information? And how should it be managed?

It is vital to be aware of information security because much of the value of a business lies in the value of its information. Dynamdre built its methodology on three essential pillars which are crucial for the success of projects of this particular nature and your business:

Confidentiality - Only the people who have a right to view it can access 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 these Information Security Guidelines may lead to disciplinary action.

Cyber crime is the biggest security threat to the modern business

"Your own personal digital defence team"

Cybercrime is hastily becoming one of the most talked-about subjects in the business world, mainly due to the drastic increase of cybercrimes and the negative impact they have had on businesses. Almost a third of the world's organisations are or have been victims of cyber-attacks, thus making cybercrime the second most common form of economic crime worldwide.

The main reason that cybercrime has increased drastically is that most companies have not yet realized its looming threat. Rather than being actively prepared and aware of the possibility of a cyber-attack, companies often choose a passive approach instead to deal with the problem. The biggest mistake anyone can make is to think that they will not become a target as studies have shown an 8% increase in cybercrimes over the past year making it the fastest growing form of the offense in the world. Cybercrime causes havoc in the finance industry and one can see the effects thereof in other industries such as mining, pharmaceutical, insurance, construction, information and communications technology, and the list goes on.

Less than 40% of organisations take necessary action to prevent a cyber-attack and its consequences, leaving more than 60% of businesses susceptible to attacks. We at Dynamdre focus our services on reducing cybercrime, and we take pride in assisting our clients in preventing this epidemic know as cybercrime/hacking, causing them financial loss or damaging their reputation.

Don't be a victim, be prepared.

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

national treasury
Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

and with the following credentials

- VAT Number: 4050 197 815
- CIPC Registration Number: 1995/051218/23
- PSIRA Registration Number: 0958804
- BEE Status – Level 4 Contributor
- SAPS Accreditation Number: 4000271
- SASSETA Accreditation Number: 051901409857
- Customs Client (Importer/Exporter) Number: 21012268 Sup
- National Treasury Supplier Number MAAA0084788

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 Naudé Road, Brummeria, Pretoria, Gauteng, South Africa, Gate 3, S25 44.874, E028 16.523