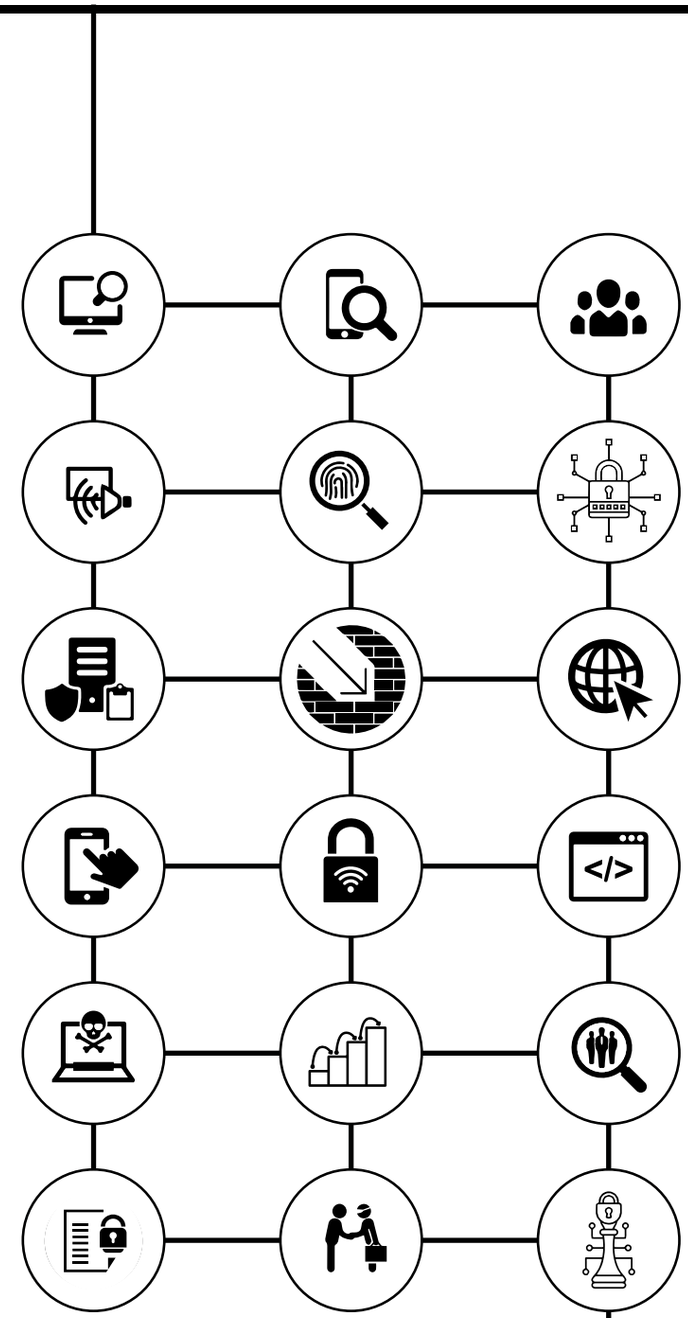
INFINITY
RISK CONTROL

YOUR TRUSTED FORENSICS & CYBER SECURITY PARTNER

CONTENTS



1 DIGITAL FORENSICS INVESTIGATION

Computer Forensics

Computer Forensics is the collection, analysis and reporting of digital data that is legally admissible. With over 98% of business having access to either a laptop or a desktop, it is expected that in nearly any type of investigation, a computer will be one of the most important source of evidence.

Computer Forensics is typically applied by isolating a user and tracking/retracing their activities for file creation, modification and deletion. Some of the most popular data files that we track or retrieve are email files. E-mail correspondence is often retrieved in these cases.

Mobile Forensics

According to global analysis firm, GSMA Intelligence, mobile penetration rates in the developed world are at an impressive 96%. People use their mobile devices as the most prominent source of communication and these devices store a wealth of data, vital to investigations. Our approach for mobile forensics, isolate the target's devices, tracks and retrace their activities to reveal incidences of data creation, modification and even deletion. For instance, a user might delete questionable data and we are able to retrieve it in its original state to build a strong case for our clients.

E-Discovery & Litigation Support

Discovery is the term used for the initial phase of litigation where the parties in a dispute are required to provide each other relevant information and records, along with all other evidence related to the case. Electronic discovery refers to discovery in legal proceedings such as litigation, government investigations, or Freedom of Information Act requests, where the information sought is in electronic format.

Social Media Forensics

Whether the platform is an instant messaging application on mobile; i.e WeChat, Whatsapp, Facebook Chat, Instagram; or a web-platform on computer, we will be able to collect, analyse, or report data files that are deleted, modified or lost.

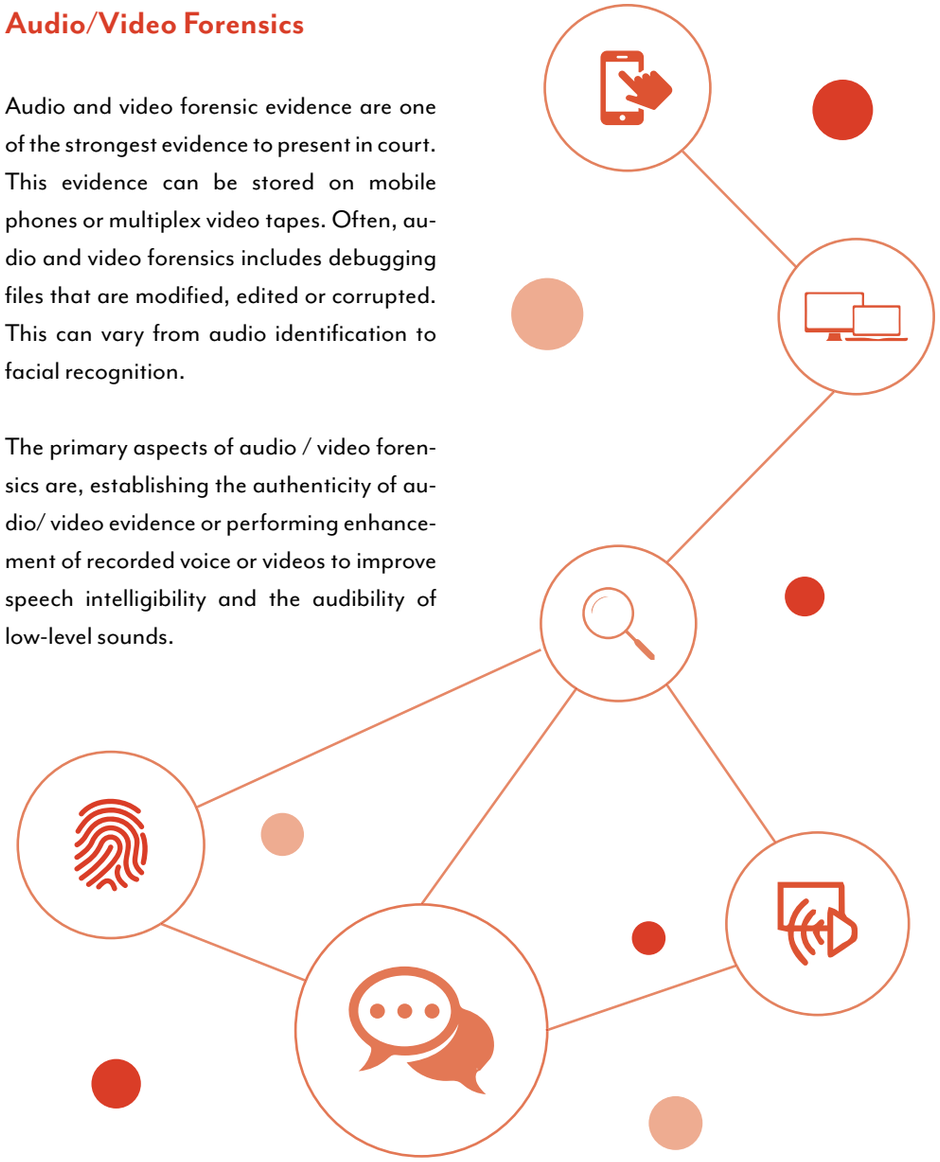
Forensics Image Analysis

Image analysis is the extraction of metadata from digital images, mainly to be used for legal purposes. Here at IRisk Control, our staffs are equipped with the skills and technology to provide tasks such from reading bar coded tags, to identifying a person from their face.

Audio/Video Forensics

Audio and video forensic evidence are one of the strongest evidence to present in court. This evidence can be stored on mobile phones or multiplex video tapes. Often, audio and video forensics includes debugging files that are modified, edited or corrupted. This can vary from audio identification to facial recognition.

The primary aspects of audio / video forensics are, establishing the authenticity of audio/ video evidence or performing enhancement of recorded voice or videos to improve speech intelligibility and the audibility of low-level sounds.



We help our clients recover and debug data from multiple sources; Computers, Mobile devices, Social media platforms, Images, Servers, Emails, and USB's. Our team has the experience and expertise to always be ready.

2

DETECTION & PREVENTION

Cyber-Security Auditing – Managing IT risks

As a business-owner, your focus is on maximizing profits. In order to continually do this, you have to manage risks that may erode at your firm's operational ability. Cyber-security is considered a prominent threat to businesses today. In order to maintain sound corporate governance, the code of corporate governance requires that all listed companies ensure that it is up-to-date on technology risks and perform annual IT risk assessments as a minimum and implement a robust programme to continually manage risk and strengthen information security controls to mitigate against the threats of increasingly sophisticated cyber criminals.

With such importance placed on managing cyber security threat to enhance company's value, we encourage you to work with professionals like us to assess your cyber security risks, based on your specific business environment and come up with the best, profit-maximizing solutions for you. This way, you can have the peace-of-mind of having a robust cyber-security system and focus on business opportunities ahead.

As we always tell our clients "Prevention is better than cure."

Vulnerability Assessment

We conduct vulnerability assessments to understand the unique context of your business operations and identify areas of cyber-security loopholes. This allows probable risks to be addressed in step 1.

Penetration Testing

A penetration test is like a "stress-test", which will simulate a cyber-attack on your system to test how your system will perform. A penetration test will consist of a simulated malicious source, an active analyses on the entire system design, a report on all operational strengths and weaknesses, technical flaws, vulnerabilities and system configurations. This allows us to identify the loopholes in the current system (don't worry, we ensure that no data is permanently lost) to act on in later steps. We also test any current risk-control measures in place to determine if it is adequate.

Web Application Audit

Over 70% of websites and web applications contain vulnerabilities that could lead to the theft of sensitive corporate data, credit cards, customer information and personally identifiable information - it is better to be aware and nip the threat in the bud.

Any lapses in security that are found are reported to the management, together with an impact analysis and proposal for technical solution or mitigation, with the findings sorted by their risk levels. It is recommendation that web application audit and review is to be performed at least yearly together with Mobile application penetration testing to ensure that the organization IT systems are constantly secure and well protected.

As Cyber-security risks increase at an exponential rate, organizations need to be on higher alert than ever. Our team minimizes the risk for organizations by offering maximum alert and attention to detail.

Mobile Application Audit

Mobile application audit is a method that allows us to evaluate the security of the mobile application by reviewing your documented security approach with the Industry Security Standards and Best Practices. It helps to clarify the security goal of your enterprise in relation to your business processes, technical systems and personnel behavior. Good internal controls in your security approach will ensure that your systems are used by the intended personnel in the intended manner, and control your legal liability.

Our cyber security consultants, who specialize in mobile application audit, will help you to identify gaps in security or technical flaws. We have the expertise to improve your controls and documented security approach.

Source Code Analysis

We provide source code analysis of your computer programs to identify security flaws in the program before it is sold or distributed. Vulnerabilities in the source code are one of the hacker's main opportunities for attacks. To prevent malicious attacks, we individually analyze applications before they are deployed and also provide safety assurance, helping you to find and fix source code vulnerabilities before they are exposed to attacks.

3 ACTIONABLE INTELLIGENCE

We provide all the intelligence to ensure that our clients are not at risk, and are always on-top.

Cyber-Threat Intelligence

We possess evidence-based knowledge, to help aid your organization's Cyber-threat intelligence. Intrusion analysis is at the heart of threat intelligence, not only will we be addressing security issues, but we will also provide actionable advice which can then be implemented within the organization to prevent it from being a victim of a Cyber-attack.

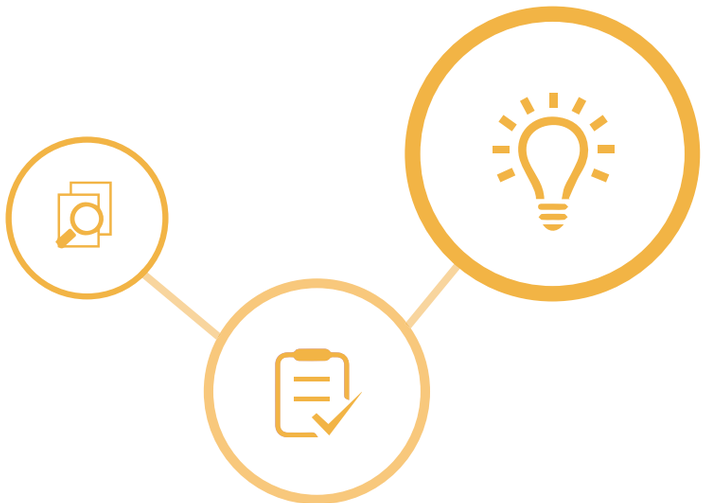
Cyber-Maturity Assessment

This is an in-depth assessment of an organizations ability to protect information assets from cyber-attacks. The assessment will educate the areas of vulnerabilities; identify areas that are in need of rectification; and nullifying cyber-risk.

Cyber Due-Diligence

A governance, process, and control that is used to secure information technology assets, turning an organizational risk into an advantage.

Instead of reacting to issues that arise, we will help you implement preventive monitored measures such as embedding a cyber due-diligence into an organization's DNA will help your organization reap rewards in the long-run.



4 ADVISORY

Corporate Cyber-Fraud

The information technology has revolutionised the way companies have operated, increasing speed and efficiency. One of the consequences is transparency. As the revolution continues to outperform itself, more opportunities have presented for malicious attackers to work under more anonymity, making it easier for corporate cyber-fraud attacks to happen. When an employee exits a company, it is essential to identify and preserve critical information that the employee possessed before it is lost forever, and to ensure that no sensitive data walked out of the door with the former employee.

Intellectual Property (IP) Theft

IP theft involves steal from people or companies of their ideas, models, creations or inventions.

This can involve a variety of reasons such as using or selling the data that is stolen from the company or individual. Sources can also vary from a competitor to an employee or ex-employee who is familiar with the system

Cyber-Security Incident Response

Incident response plans provide instructions for responding to a number of potential scenarios, including data breaches, denial of service/distributed, denial of service attacks, firewall breaches, virus or malware outbreaks or insider threats. This is an organised approach to a cyber-security issue that was pre-prepared for the incident, for the duration and the aftermath. The mission is to handle the issue, prioritizing damage limitation and reducing the recovery time so that an organization can operate at maximum efficiency in the given situation. Without an incident response plan in place, organizations may either not detect the attack in the first place, or not follow proper protocol to contain the threat and recover from it when a breach is detected.

Strategy and Governance

Creating and following a set of strategies to governance the performance of a body so that maximum efficiency can be achieved through carefully planned preventive and responsive measures.

Our team will work hand-in-hand with your team to ensure that you will not only avoid any cyber-threats, but also have a competitive advantage in the market.

ABOUT

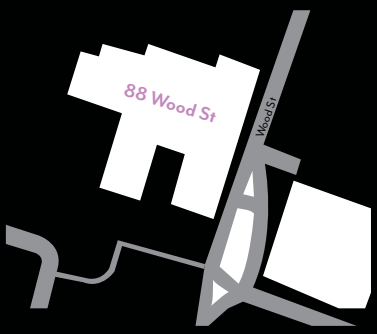
Infinity Risk Control (IRisk) is a Cyber Security industry leader in South East Asia based in Singapore and London. Founded in 2006, IRisk has been in the market for over 10 years, boasting a clientele that involves over 16,000 consultations, with a variety of partners, including, government agencies, private institutions, MNC's and private individual cases.

IRisk services include Computer Forensics, Mobile Forensics, Digital Fraud Investigation, Vulnerability Assessment, Penetration Testing, Wireless Security Audit, Actionable Intelligence, Cyber Threat Intelligence, Malware Analysis and eDiscovery & Litigation Support.

With innovation being central in modern economy, adaptability becomes vulnerability. Here at IRisk, our professional staff are constantly updated with the exponential changes, giving them the ability to provide quick and precise response times.

LONDON

88 WOOD STREET, 10TH -11TH FLOOR
GREATER LONDON
EC2V 7RA / UNITED KINGDOM
PHONE: 44 203 6953536
EMAIL: INFO@IRISKCONTROL.COM



SINGAPORE

35 TANNERY ROAD #09-05
RUBY INDUSTRIAL COMPLEX
344440 / SINGAPORE
PHONE: 65 68460654
EMAIL: INFO@IRISKCONTROL.COM