Introduction to information security and cybersecurity, and a summary of the services and software solutions offered by Kiowa Security

Robin Long (Founder, Kiowa Security Ltd)
June 2023

PART ONE: INTRODUCTION TO INFORMATION SECURITY AND CYBERSECURITY

1. Background

i. Sensitive Data

'Sensitive Data' refers to information the compromise of which could cause problems for the organisation that is managing it.

'Managing data' might mean using it for normal business activities, storing it or processing it on behalf of another organisation. 'Compromise' of Sensitive Data means a failure of Information Security of the data, as defined in the following sub-section.

Due to the high profile of data protection regulations like GDPR, Sensitive Data is widely believed to refer only or largely to Personal Data that might be used to identify an individual. However, Sensitive Data also includes:

- Unpublished Intellectual Property (protected creative output that has not yet been made publicly available, such as source code, written documents and artwork)

- Trade Secrets (commercially valuable information that is known only to a limited number of people – for example corporate strategy or financial accounts)

- Official Secrets (information that is important for national security)

- Industrial Control System data flows that are used for monitoring and management of processes in industry, energy and transportation.

- Private keys, authorisation tokens and other pieces of information that underlie cryptographic activity, for example around cryptocurrency transactions.

Obligations regarding Personal Data are mainly due to data privacy regulations (GDPR, CCPA etc.) and most larger organisations base their data protection policies – if they have any - on GDPR. This is partly because they are normally exposed to EU or UK data in one way or another, but also because non-European data privacy legislation (for example, in China and S. America) is nearly always very similar to GDPR.

Other types of sensitive data are protected by legislation such as the UK Official Secrets Acts (1911-1989), industry standards, bilateral contracts like Data Protection Agreements and NDAs etc.

ii. Information Security

'Information Security' refers to the protection of Sensitive Data from three main types of compromise: Failure of

- **CONFIDENTIALITY** (unauthorised access to data)
- **INTEGRITY** (unauthorised modification or deletion of data)
- **AVAILABILITY** (users can't access data normally)

iii. Cybersecurity vs Information Security

Information Security refers to protection of Sensitive Data against the above types of compromise regardless of the form of the compromise (i.e., not necessarily just electronic 'cyber' compromise). For example, if paper documents containing Personal Data are damaged due to flooding, then that's an integrity compromise like any other. Equally, if trade secrets are revealed because someone talks about them loudly in a restaurant, then that's a confidentiality compromise as surely as if they'd been stolen by a hacker.

Cybersecurity is about IT hardware, software and data in electronic form and is a subset of Information Security, albeit one that has almost filled the entire space of Information Security, as organisations have shifted storage and processing of data to computers.

However, non-cyber aspects of Information Security remain important, in particular:

>> Human resources (HR) security
>> Behavioural security around remote working
>> Physical security (doors/keys, fire protection, CCTV etc.)
>> Compliance with legal, regulatory and contractual requirements
>> Project and change management
>> Business Continuity and Disaster Recovery

If HR security is weak (people in sensitive roles aren't properly screened, security responsibilities aren't covered in employment contracts, etc.) then many measures that are typically deployed to protect Sensitive Data are rendered ineffective or less effective, as employees ('insiders') are often able to evade them much more easily than outsiders.

Information Security may be compromised not only due to malicious activity by an external adversary (e.g., a ransomware group), but also as a result of misconduct or negligence by an insider. The concept of the 'insider threat' is one that people tend not to like much, but it is a real one that should be an important consideration in any organisation's approach to Information Security.

Sensitive Data can of course also be disrupted by natural events; fire, flooding, earthquakes etc.

2. Threats – who or what is the enemy?

i. External Adversaries

- **Ransomware gangs**
  The groups that attack organisations with ransomware malware. This type of attacker is the one that deserves the most attention.

- **Financial fraud gangs**
  Similar to the ransomware gangs but focused on financial fraud - sophisticated BEC (Business Email Compromise) scams that can result in a large, unauthorised transfer of money out of the victim organisation, which can be almost impossible to retrieve.

- **Advanced Persistent Threat (APT) groups**
  Coordinated teams of highly trained, experienced hackers that are supported by nation states. Normally the link between the hacking group and the nation state that sponsors it is intentionally blurry in order to avoid attribution.

  These are the most sophisticated and well-resourced adversaries. They undertake espionage operations and attacks on critical infrastructure, and in some cases (particularly N Korea) they are self-financing via cryptocurrency hacks.

  Many countries have officially-recognised elements of their armed forces and intelligence that conduct cyberoperations, but these are mainly focused on defensive activity. Aggressive cyber activity is normally done by APT groups – especially if it's legally questionable.

  Do most organisations have to worry about APT groups? Not really.

- **Hacktivists**
  Politically motivated hacking groups.

- **Opportunists and loaners**
  Old-style hackers. They tend to use unsophisticated techniques and hacking tools that they purchase online to disrupt businesses or steal money from them and their customers.

ii. Insiders

Employees and other insiders can be a problem for Information Security due to the access that they have to sensitive data. That power can be turned against the business if they become unhappy, or are careless, poorly trained or corrupt.

They might:

- Delete or modify data by mistake
- Steal data and exfiltrate it by email/upload to cloud storage/IM/USB key/printing/photo with mobile phone/memorisation…
- Intentionally or unintentionally giving access to an attacker (click on link in email/reveal password/respond to bribery…)
- Damage hardware

iii. Natural Events

Data may be disrupted by natural events that cause damage to buildings, hardware, communications channels etc.

3. Threats – how is Information Security compromised?

i. Unsophisticated attacks

Isolated, straightforward attacks that require little to medium expertise. In some cases they can be implemented by someone with no cybersecurity knowledge whatsoever, that simply purchases the attack from some other hacker on the dark web "Crime as a Service/CaaS".

Just because these attacks are unsophisticated doesn't mean that they can't do serious damage, or cause substantial financial losses.

- **ATTACKS ON WEB APPLICATIONS**

  The attacker exploits vulnerabilities in a sensitive web application such as a banking site, crypto exchange or gaming platform. By doing this, they may be able to take over customer accounts, access the back end of the web application (where information such as private keys may be stored) or compromise data in other ways.

- **DENIAL OF SERVICE (DOS) ATTACKS**

  The attacker sends so much data or requests to an IT resource such as a server, network or web application that it cannot cope and fails to operate normally. This can cause compromise of availability of data, for example by preventing banking customers from accessing their accounts.

DoS attacks are normally carried out by a coordinated group of infected computers (a BotNet), in which case they are called Distributed Denial of Service (DDoS) attacks.

ii. Sophisticated, multi-vector attacks.

This type of attack is exemplified by ransomware; it is carried out by a group of people that have a high level of hacking expertise. Contributory elements to the attack are likely to include a reconnaissance phase, development of tailored malware and other stages of what is known as the 'cyber kill chain' – described in a later section of this document.

- **RANSOMWARE**

  Ransomware attacks entail coercion of the target organisation ('victim') to give money to the ransomware group, normally according to this sequence of activities:

  1. Break into the victim's device(s), IT network and/or data storage (perhaps in the cloud)
  2. Find and then encrypt the victim's sensitive data where it is currently being stored, using a private encryption key that's unknown to the victim.
  3. Notify the victim about what's happened, telling them that they must pay a cryptocurrency ransom to some anonymous account

  Variations on this theme include:
  - Actually stealing data by exfiltrating a copy of it and deleting the victim's version
  - Threatening to publish sensitive data
  - Adding extra pressure by attacking the victim's website with DDoS attack, threatening to inform shareholders and customers, etc. ('double extortion')
  - Attacking backups of data so that the victim can't restore encrypted or deleted files

- **BUSINESS EMAIL COMPROMISE (BEC)**

  The attacking group develops relationships with key staff in the victim's organisation using social media and emails that appear genuine but are in fact created using hacking tools and techniques. Targeted employees might be treasury staff, HR, and senior employees like the Finance Director, CFO or CEO.

  Once they've established trust and done their groundwork, the group carries out its attack. This is normally done by sending an email to a treasury operative in the name of the CEO or CFO, instructing a large bank transfer. The email will pile on the pressure, often be sent at a time that is close to the close of business, and be supported by phone calls and text messages.

- **ESPIONAGE**

  Theft of sensitive data; similar to the initial stages of a ransomware attack but targeting critical infrastructure operators, government bodies etc. and done by APT groups using sophisticated tools and methods.

- **ATTACKS ON CRITICAL INFRASTRUCTURE**

  The corporate IT network and assets are infiltrated by the attacker, who then proceeds to traverse from that network to the OT (Operational Technology) network. This is where ICS (Industrial Control) and SCADA systems are managed; once a skilled adversary has gained access to these, they are in a position where they can trigger failures in the supported processes. Gas networks, refineries, water treatment works, steel production facilities and so on can be disrupted and even permanently damaged in this way.

iii. Insider threats

- The scope of malicious attacks by insiders is limited only by what access the insider has (not only in terms of information that they can view, but whether they have rights to copy or modify data). Clearly insiders also have access to hardware, so they can steal or deliberately damage desktop computers, laptops, routers, printers…

- Insiders can also cause compromise of Sensitive Data due to negligence and in fact this is more frequent than intentional theft or disruption.

  That might mean:

  - Negligently revealing access credentials (user name, password) or other Sensitive Data – for example by allowing someone to see their laptop screen in an airport lounge.
  - Losing hardware or failing to protect it properly, so that it gets stolen
  - Sending sensitive data by email to the wrong person by mistake
  - Misconfiguring software and particularly cloud storage services
  - Deleting files by mistake

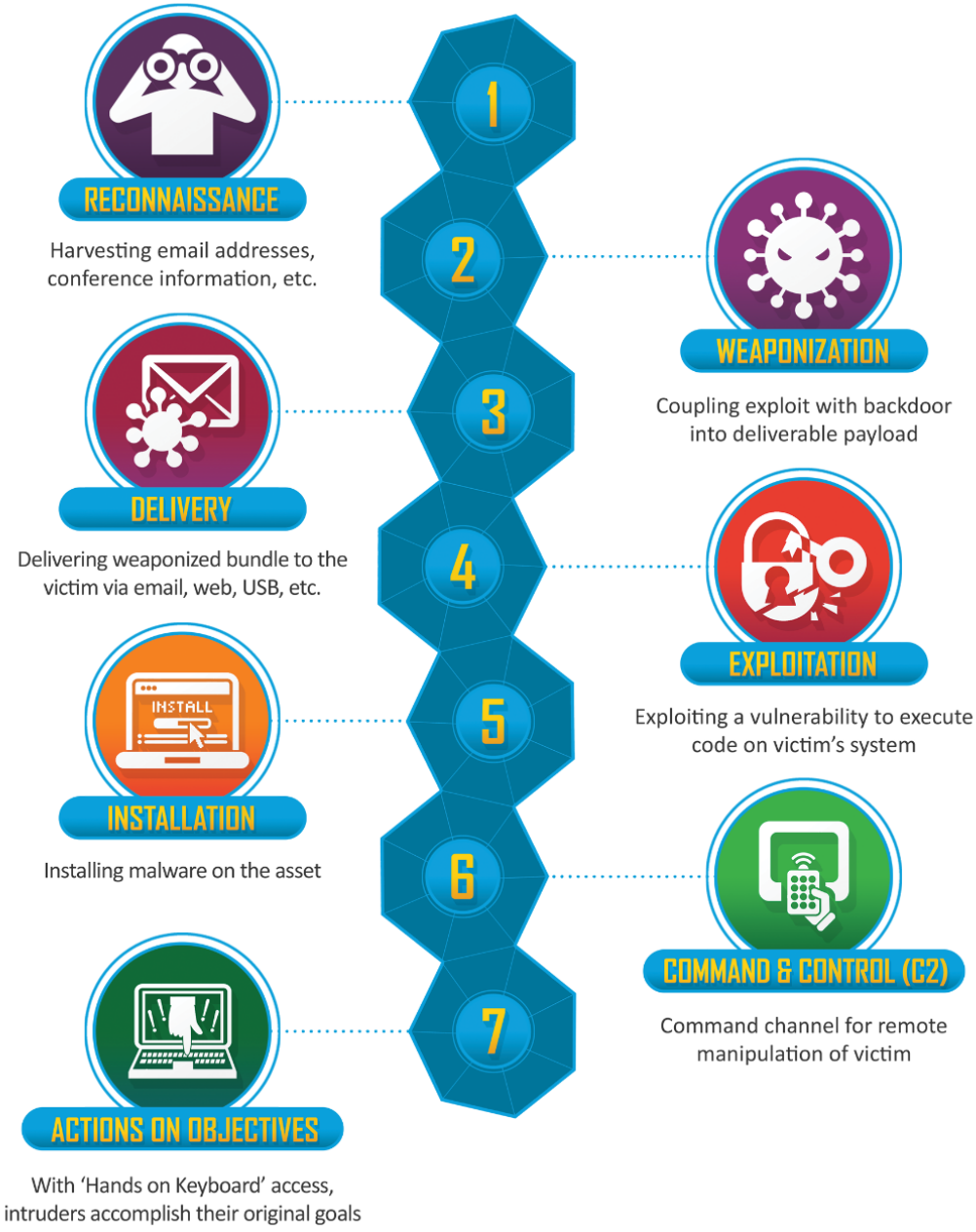
iv. Risks from natural events

'Natural events' refer to fires, floods, earthquakes, hurricanes and other phenomena that are normally outside human control. Mice chewing through cables is genuinely a potential risk that needs to be addressed by some organisations.

If an organisation is exposed to these types of risks, then potential impact on Information Security includes effects resulting from damage to:

- hardware that is used to store or process Sensitive Data
- hardware that is used to support transmission of Sensitive Data (routers, cables..)
- utility infrastructure, particularly electricity and internet
- transportation and buildings (preventing employees to get to work or to work normally)
- data centres

Risks of this type are largely mitigated by the business continuity/disaster recovery plan, which in turn leans on redundancy and failover for critical assets and services.



Infographic: Cyber Kill Chain (developed by Lockheed Martin)

4. Carrying out a cyber attack

i. The Cyber Kill Chain

Most sophisticated attacks follow the following sequence of phases:

1. Reconnaissance (find out about the target organisation using software and old-fashioned social engineering)
2. Weaponization (build appropriate malware 'virus' package)
3. ***Delivery*** (get the payload into the victim's device and network – again, using social engineering techniques such as phishing)
4. Exploitation (trigger the malware within a device)
5. Installation (install a backdoor within the victim's network)
6. Command & control (malware opens up communications with an external server)
7. Actions on objective (look for sensitive data and encrypt, delete and/or exfiltrate it, or whatever other aims the attacker might have)

Note that:

- An attack can be caused to fail by disrupting it at any step of the cyber kill chain (the above phases)
- Cybersecurity solutions (technical or procedural measures used to mitigate cybersecurity risks) tend to focus on doing exactly that (email security, file scanning, detection of suspicious network activity, detection of attempts to send data out of the network etc.)
- The Delivery phase is a particularly important and vulnerable step of the chain. If employees can be trained to spot phishing emails, then many attacks can be prevented at this stage.

ii. Attack Vector

The Attack Vector (AV) is the method used to insert malware into the victim's network during the Delivery step - a very vulnerable phase for the attacker.

Even highly sophisticated attacks tend to use social engineering techniques and phishing emails as the AV in the Delivery phase of the kill chain. For some reason, that aspect of hacking has not evolved much in recent years, although the quality of phishing has definitely improved.

Phishing emails and text messages look bona fide. For example, they might look like genuine messages requesting personal information from Amazon or Parcelforce. However, the attachment or website link that they contain trigger a download of malware onto the user's device.

Alternative AV's include attacks that leverage security misconfigurations and vulnerabilities in web applications, and attacks on VPN/remote desktop.

iii. Malware

"Malware" = Malicious Software. Once installed in a device it carries out some or all of steps 5-7 in the cyber kill chain. These might include:

- Logging keyboard activity (e.g., for passwords, credit card credentials)
- Searching around the network for sensitive data
- Exfiltrating/encrypting/deleting data, or some combination of these.
- Establishing communications with an external server, which can provide instructions or install additional malware
- Taking partial control of the device in order to do unauthorised crypto mining or participating in a DDoS attack

iv. Vulnerabilities

All operating systems, software, firmware and devices have some kind of vulnerability or vulnerabilities in them that can be exploited. That means a weakness that an attacker can take advantage of in order to access the asset or do other unauthorised activity. We may not know about them yet, but they're there – nothing is perfect, even in military systems! It's just a matter of how long it takes for an adversary to find them.

Once a vulnerability is discovered by – or communicated to – the organisation that is responsible for it, then that organisation will normally issue a security update/patch. For example, every time that Apple releases an OS update for iPhones, iPads and Macs, it contains security updates to patch found vulnerabilities.

Meanwhile, attackers start looking for and exploiting found vulnerabilities straight away, and also share details about them with other hackers using the dark web.

It is often possible for adversaries to scan the internet for exposed devices that are using software/firmware versions that are out of date and vulnerable to recently discovered exploits (for example early versions of Windows OS).

Organisations can enrol in 'bug bounty' programs whereby they commit to making cash payments to ethical ('good guy') hackers that spot vulnerabilities and other coding errors ('bugs') and notify them. This is definitely recommended.

v. Zero Days

When a type of malware is created that has never been seen before, it can be hard for cybersecurity solutions to manage. This is because most anti-malware software is based around a library of signatures of malware instances that have been spotted and documented. Probably around 99% or more malware is in the

documented category – the remaining 1% tends to slip through standard protective software.

Zero-day malware can sometimes be detected by software that uses techniques such as sandboxing (launching or 'detonating' suspicious files in a controlled environment to see what they do) and machine-learning approaches that look for very subtle signs that a file may be malicious.

Vulnerabilities that have just been discovered, and for which a security update has not yet been released are also described as zero days. They are also a major problem: Attackers that become aware of them will use them as quickly as possible against their most attractive targets, and try successfully to exploit them before victims can roll out security updates. This is why security updates should always be deployed ASAP.

vi. Misconfiguration of security settings

This occurs when the victim fails appropriately to configure the security settings of exposed resources. For example, they might set up a cloud storage resource containing sensitive data such that it can be viewed publicly with no password requirement. This happens surprisingly frequently.

Misconfigurations of this type can often be detected by scanning software and specialised search engines. They are an inexcusable reason to be hacked.

vii. Password or login attacks on web applications

An important family of attacks on web applications leans on vulnerabilities around passwords and logins. These vulnerabilities might be in the web app itself, or due to users managing their passwords badly.

POOR PASSWORD MANAGEMENT BY USERS

Users can expose themselves to unnecessary risk by failing to choose and manage passwords correctly, in two main ways:

- Choice of passwords that are too short, insufficiently complex and too easy to guess (e.g., 'password', 'robin123', aaaaaa etc.)
- Using the same passwords in different places (for example, same password for Gmail, Amazon, LinkedIn, Zoom etc. This is one of the main risks for users, as it exposes them to the 'Credential Stuffing' attack that is described below.

TYPES OF ATTACK ON LOGINS AND PASSWORDS

Brute Force Attack; Dictionary Attack
In both of these attacks, the adversary attempts to guess the user's password by trying all or many of the different possible ones. This might be billions, trillions or more permutations of letters, numbers and special characters.
In a brute force attack, the attacker works through all different possible permutations including completely random selections.

Dictionary Attacks use popular known passwords, names and real words, so they can often crack the password much more quickly than pure brute force.

Passwords are more resistant to these attacks if they are longer, use a combination of letters, numbers and special characters (like $, &, @) and are random selections rather than real words or names. Minimum should be 8 or 10 mixed character types.

Credential Stuffing Attack
From time to time, attackers successfully hack an organisation and steal the database of usernames along with their associated passwords. Once they have these, then that organisation's user accounts are obviously vulnerable.

However, the attacker is also able to take advantage of the fact that users often use the same passwords in different locations. They do that by testing these found username/password combinations on other web applications; when an organisation is severely breached, affected users often find that accounts that they hold elsewhere are also attacked.

This risk is mitigated by users being careful not to use the same password for different applications – best achieved by using a password manager.

MULTI-FACTOR AUTHENTICATION (MFA)

Most password/login attacks can be mitigated by the use of 2FA (two factor authentication) aka MFA. This is described in a following section.

5. The dark web and cybersecurity

The dark web is used by a number of different participants of the cybersecurity ecosystem, and does need to be taken into consideration as part of overall information security. This is because it is contains forums and market places for display of and trade in:

- **Data that's been stolen in ransomware attacks**
  Ransomware gangs often display stolen data on forums and specialised websites, to prove that they have been able successfully to hack their victims, and to put pressure on them.

- **Stolen information that might be used by attackers**
  Stolen usernames, credit card credentials and other sensitive data often turn up on dark web forums and market places. That might be the first sign that your business has been hacked.

- **Cybersecurity goods and services**
  Malware and found vulnerabilities including expensive zero-days are available for sale on the dark web. That means that cybersecurity threat researchers and law enforcement operatives spend a lot of time looking at what's available there, and trying to work out who's selling it!

Law-abiding organisations make use of software and service suppliers that monitor the dark web, looking for information that may be relevant for them.

6. Defensive concepts in information security and cybersecurity

• The attack surface

This is the totality of all the different points via which an adversary might be able to access your organisation's sensitive data. This includes:

- Devices
- Websites and apps
- Corporate WiFi access points
- IoT devices (connected CCTV, HVAC etc.)
- Employees
- Suppliers and SaaS with access to data
- etc. etc…

One primary objective of any Information Security plan is rigorously to map out the organisation's attack surface. In ISO27001 this is done by creating an Asset Inventory which lists out assets that are related to information security, and assigns an owner to each of them.

"An organisation's Information Security is as strong as the weakest point on its attack surface".

A small attack surface is more secure than a large one, but there is a trade-off between attack surface size and freedom of information flow that may cause problems for some organisations.

Once the attack surface is well understood, it should be gap tested for risk-assessed protection on all its points and any failures remediated.

- **Defence in depth**

  This is a defensive strategy that was developed in medieval times and is now used – obviously in adapted form - in Information Security.

  The basic concept is that multiple layers of security are much harder to penetrate than a single layer, rather like a medieval fortress with a moat, outer walls, keep etc. In Information Security this is expressed by deployment of a series of layers of defensive measures, e.g.,

  >> Employees are screened and given security awareness training
  and
  >> Emails are scanned by a software solution
  and
  >> Anti-malware software is installed on computers
  and
  >> Sensitive data are encrypted and securely backed up

  To quite a great extent, defence in depth responds to the cyber kill chain representation of a typical sophisticated cyberattack.

- **Zero Trust**

  The Zero Trust approach to cybersecurity has arisen largely due to the change in typical corporate network architecture that has happened in the last ten years or so. This, in turn, has been driven by a shift of data and applications to the cloud, and the prevalence of remote working:

"Traditional" architecture	"New "architecture
Data stored on server(s) in the office	Data stored in the cloud
Applications operate within the perimeter	Applications regularly cross back and forth over the perimeter
Users normally work in the office	Users work all over the place
Users VPN into servers	Users connect to cloud services over the internet
Applications, data and users in an organisation mainly communicate within the same country	Organisations often regularly see communications and data flows that are between countries and even intercontinental
Sufficient to apply most security at the perimeter (network firewall)	Network firewalls don't make any sense anymore and users and applications must be authenticated wherever they may be

  The Zero Trust approach to security (Zero Trust Architecture) engages with the "new" Cloud/Remote Working architecture, and ideally combines the following features:

- Continuous verification and authentication of 'agents' - human users or applications - using multiple attributes that might include user identity and credentials, geolocation, device type, patching level, time etc.
- Minimum required access, provided only when its needed
- Secure encryption everywhere!
- Verification of software and hardware
- Continuous monitoring of log data
- Network segregation to prevent adversaries moving around

Several software solutions have been developed that can enable businesses to implement some kind of zero trust approach.

- **Multi-factor authentication (MFA)**

Traditionally, authentication and access control into devices and applications has been via a login process that uses one 'factor'. A factor is something that only the correct user should have access to – for example, a password/PIN, card, fingerprint. We have seen that passwords are quite vulnerable, but this can also be the case for physical keys (which can be lost or stolen) and other single factors. By using two factors rather than one, the level of security can be very substantially enhanced.

Most people are familiar with MFA nowadays (typically implemented as 2FA, with just one additional factor). The most popular second factor is currently an OTP (one time password) that is sent by SMS or email, or generated by an authenticator app.

MFA is becoming a requirement for the protection of sensitive data, as single-factor authentication using passwords is now so frequently abused.

- **Threat intelligence**

This is about staying on top of the latest threats, risks and trends in cybersecurity. Organisations are recommended to make certain employees (typically the Information Security Officer) responsible for subscribing to reporting services that provides updates about information security, cybersecurity and data privacy regulations. Other suggested sources include a range of websites, Twitter, LinkedIn and so on.

These responsible individuals screen, sift and share relevant information that they have picked up with other employees, in a way that may be formalised (e.g., weekly newsletter, ad-hoc alert emails messages).

7. Information Security Standards and Frameworks

Given how many aspects there are to Information Security and cybersecurity that apparently need to be addressed, you may well ask how an organisation can verify that it has an approach in place that is sufficiently rigorous, complete and effective.

Secondly, how can it provide evidence of this to third-parties that are looking to do business with them or invest in them?

A good response to both of these questions is to get a certification or attestation to a recognised and respected security framework.

The main ones are ISO27001, SOC2 and NIST CSF. An increasing number of organisations – particularly government/council, finance and critical infrastructure, although the list is growing – require suppliers that access their sensitive information to have one of these.

The process to obtain one is roughly as follows:

1. Conduct a gap analysis of the organisation's level of information security in all areas of the certification, vs the requirements of the certification
2. Conduct a risk assessment based on the above
3. Do whatever is required to meet the certification requirements based on the gap analysis and risk assessment (write up documentation, establish processes and procedures, assign roles or hire staff, purchase software etc.)
4. Conduct an internal audit to verify that conditions have been met
5. Either get certification audit done (ISO27001) or write attestation (SOC2)

Depending on the size of the organisation, it can take between about four months and a year to achieve ISO27001 certification. Then it must be recertified on an annual basis.

8. HR security

Human resources security is such an important part of information security that it merits its own section in this document. HR security means a lot more than screening – here are the main components:

- Screen employees (DBS check, CV verification, references)
- Ensure that Information Security is properly covered in the Employment Contract and Employee Handbook, including correctly worded confidentiality clause/NDA
- Ensure that employees receive regular security awareness training and keep a record of their performance
- Do other training/education (GDPR, secure development…)

- Have in place a disciplinary procedure process; it should include definition of negligence, misconduct around information security responsibilities
- Follow onboarding/offboarding procedures for new starters and leavers

9. Secure Development

Organisations that develop software that is exposed over the internet (largely, web applications) need to be very careful that the software is written and built securely: Attackers have 24 hours/day, 7 days/week available for scanning and investigation of websites to look for exploitable flaws, and they use this time productively.

Core aspects of Secure Development include:

- Having a policy in place regarding secure development
- Following a Secure Software Development Lifecycle (SSDLC)
- Establishing software engineering principles that must be applied by developers
- Ensuring security of development environments by using appropriate access control policies and technical measures
- Using software to:
  - Analyse open source components and container images
  - Do static analysis of written code to check for vulnerabilities
  - Check licensing conditions of open source components

10. Business Continuity, Disaster Recovery and Incident Response

These practices and procedures are highly relevant to Information Security, and vice versa.

Approaches to Business Continuity and Disaster Recovery have changed considerably now that so many more employees work remotely – or can easily do so if necessary. For example, organisations nowadays tend to worry less about physical disruption (natural disasters, fires etc.) and more about appropriate configuration of cloud services in terms of backups and redundancy.

Critical SaaS providers are also in the spotlight: How well designed and tested are their own BC/DR plans? Are alternative suppliers available if one goes down (supplier redundancy)?

Business Continuity
This is the practice of maintaining normal business operations if some kind of disruptive event occurs. The relevance to Information Security is largely due to the risks of compromise of availability and integrity of Sensitive Data for clients, employees and third parties.

It's also critically important that Information Security of data is maintained despite adverse circumstances that might include employees being forced to work

remotely, fewer senior employees being available, failure of certain communications channels, loss of critical suppliers and so on.

Incident Response
This is about how the business reacts to a compromise or potential compromise of Sensitive Data, such as a ransomware attack or theft of data by an employee. The quality of the response by employees may determine whether or not the business survives a major incident.

Disaster Recovery
This is regarding getting the organisation back to BAU status as soon as possible after a disruption event. It is largely concerned with employees being familiar with the procedures required to return assets and services to normal operation, but also failovers/fallbacks and how to get them up and running.

11. Data protection regulations, for Personal Data

Here's a brief summary of the main requirements of GDPR; most national or state-level data protection legislation is modelled to quite a great extent on GDPR, and GDPR is directly relevant to a lot of organisations anyway, due to the fact that so many businesses control or process at least some data that is associated with EU or UK nationals.

*'**Personal Data**' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

*'**Processing**' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

*'**Controller**' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law*

*'**Processor**' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*

- **INFORMATION SECURITY**
  Personal Data should be protected against accidental loss, destruction or damage, using appropriate technical or organisation measures.

Confidentiality, integrity, availability and resilience of processing systems and services must be ensured.

- **DATA BREACHES**
  Subject to certain conditions, any data breach must be notified to the relevant regulatory authority within some statutory period.

- **RIGHTS OF THE SUBJECT**
  [The 'Subject' is the person that the personal data is linked to; the owner of the data]
  Personal Data should only be collected for good reason and in a transparent fashion.
  Personal Data should not be retained for any longer than necessary (data retention policy, data discovery and deletion)
  The Subject has the right to access, rectify or erase the data ('right to be forgotten')
  Subjects should normally be informed 'without undue delay' if their data has been compromised.

- **CONTROLLER AND PROCESSOR**
  The different specific obligations and requirements of Controllers and Processors of Personal Data

- **DATA TRANSFER ACROSS BORDERS**
  There are strict controls regarding Personal Data moving outside or into different jurisdictions. This is highly relevant for organisations that use cloud services that host data over multiple data centres.

- **PENALTIES THAT MAY BE INCURRED DUE TO A DATA BREACH**
  Description of the fines and other penalties that may be applicable to infringements of the regulation.

- **PRIVACY POLICY**
  There must be a publicly available Privacy Policy that shows, among other things:

    - Contact details of data controller
    - Information that is retained and why it is retained
    - How long it's retained
    - Statement regarding security measures that are in place
    - Statement regarding the subjects rights regarding access, rectification, erasure and complaints
    - Contact details of relevant regulator

PART TWO: SERVICES AND SOFTWARE SOLUTIONS OFFERED BY KIOWA SECURITY LTD

1. ISO 27001

Kiowa can support the journey to achievement of ISO27001 in the following ways:

i. Gap analysis of the organisation's Information Security based on the ISO27001 controls
ii. Information Security risk assessment
iii. Drawing up of asset inventory and data inventory
iv. Implementation of ISO27001
v. Internal audit for ISO27001
vi. Arrange certification audits and coordinate with assessing auditor.

A sensible alternative to attacking the whole of ISO27001 as a single project is to break it up into manageable pieces, put them in order of priority and work through them one by one. This might look something like:

1. HR Security
2. Access Control
3. Secure development
4. Business Continuity/Disaster Recovery
5. Compliance with rules and regs
6. …

2. Penetration testing

Penetration testing ('pen testing') refers to testing during which an authorised attacker without access rights attempts to access an organisation's sensitive data.

Depending on the type of testing that has been scoped, the tester may:

- Have more or less initial access (i.e., they may or may not know IP addresses, be allowed to use VPN etc.)
- Start at the beginning of the attack chain (initial access at the 'Delivery' stage via e.g., phishing) or later in the chain
- Use a combination of automated and manual tools

Kiowa has partnerships with two pen-testing companies; basically one is cheap and one is expensive. Kiowa can set up the introductory calls and help to coordinate actual penetration testing.

Bug bounty programmes also make a lot of sense for organisations that are sensitive about security like crypto exchanges, and Kiowa can also help with that.

3. Software solutions

Selection and deployment of software solutions is obviously important and can be expensive, so it needs to be done correctly. There can be serious security problems if errors are made.

Kiowa can assist with software solutions in the following ways:

i. Provide advice regarding types of software solution that are recommended given gap analysis and the organisation's goals and priorities in Information Security
ii. Present a shortlist of potential solutions that appear appropriate given criteria that include:
    - Precise required functionality
    - Number of users
    - Available support staff
    - Budget
iii. Arrange product demo, technical calls and POC (Proof of Concept testing) if necessary, and assist in making final decision
iv. Negotiate contractual terms with vendor
v. Assist with deployment of the software

4. Available software solutions

These are currently the main available cybersecurity software solutions, although it is not an exhaustive list and there are many more specialised solutions that may be appropriate for specific use cases.

i. Endpoint protection (EP)

This is effectively anti-virus software for corporate computers. EP software nowadays offers some or all of these functions, several of which are well outside the scope of 'anti-virus':

Minimum requirements:

- Scans attachments and other files for malware
- Checks websites against blacklists, and checks URLs
- Scans web downloads for malicious content

Additional possible functionality:

- Scans emails and attachments to mitigate phishing attacks (email security)
- Provides some level of protection against zero day attacks (typically done using sandboxing or machine learning)
- Controls data going into and out of USB ports
- URL filtering (block access to known or suspected malicious websites)
- Disk encryption on the device

Corporate EP solutions are managed from a centralised platform in order to ensure that the software running on all devices is configured according to the organisation's policies, and is active. Employees don't normally have rights to modify the settings of the EP on their devices.

Endpoint Detection and Response (EDR) and **Extended Detection and Response (XDR)** are forms of endpoint protection that centralise and analyse data from all endpoints to look for network-wide anomalies and other evidence of stealthy attack. EDR/XDR (like SIEM, below) is a tool that requires management by a specialised team of security staff (Security Operations Centre, SOC).

With **Managed Detection and Response (MDR)**, there is no need for additional staff to monitor the output of the EDR; it is managed by an external company.

ii. Mobile Device Management (MDM)

This enables centralised control of employee devices, with four main objectives:

- Ensure that devices are correctly configured and up to date in terms of Operating System and other software and security updates
- Prevent employees installing unapproved software
- Manage data flows out of the device (i.e., prevent employees doing unauthorised exfiltration of sensitive data by email, upload to cloud services etc.)
- Remote protection of data in the event that a devices is lost/stolen/no longer needed etc. This might be via complete device reset or selective deletion of data.

iii. Data management solutions including discovery tools and Data Loss Prevention (DLP)

These solutions are largely about regulatory compliance with data protection regulations such as GDPR, but are also used to mitigate the risk of Insider Threat (intentional or accidental exposure of sensitive data)

- Data discovery is concerned with working out exactly what sensitive data you have and where it is stored. This might be on company computers and servers but also on cloud-based systems.
- DLP tools monitor data that is being transmitted out of the organisations assets. This might be by email, IM, upload to cloud services or even printing.
- The solution is configured to be familiar with what the organisation defines as Sensitive Data, which might include addresses, phone numbers, credit card credentials, passport numbers and also IP such as written code (which is easily identifiable).

- The DLP software reacts when it observes attempted exfiltration of Sensitive Data. Depending on the type of data, it may simply block and report, or it might enforce encryption of the data, among other management options.

iv. Web Application Firewall (WAF)

- Just as networks and devices may have firewalls that control data traffic that passes through them, so can web applications.

  [What's the difference between a website and a web application?]

  A website is one or more static pages that can be viewed over the internet. 'Static' means that users can do no more than view content, images, video etc – they can't interact with the pages and cause the content to update dynamically. If they need – for example – to make a payment to the website, then the user is taken elsewhere (in fact to a web application as described below).

  Web applications are websites that are interactive and functional. They may have forms, chatrooms, payment mechanisms and so on, and normally they provide access to information that is stored in a database (the 'backend'). Banking websites, crypto exchanges and retail websites are examples of web applications.

- Web application firewalls protect web applications against malicious traffic that is directed against them over the internet, such as:

  - DDoS attacks where the adversary attempts to overwhelm the web application with requests, and prevent it from operating normally

  - Exploits of vulnerabilities in the web application that are due to insecure design or software development

  - Malicious activity by 'bad bots' (software applications that pretend to be human but perform undesirable activities like arbitraging betting odds, or scalping tickets)

- The WAF works by inspecting data packets that are sent to the website. The organisation that suppliers the WAF (e.g., Cloudflare) has massive computing resources; it intercepts the data packets, decrypts them, analyses them and then either forwards them on or blocks them. Companies like Cloudflare are large enough that they can and regularly do absorb huge denial of service attacks that are directed at their customers.

v. Zero Trust Network Access (ZTNA)

ZTNA is a software implementation of one aspect of Zero Trust; it does this:

- Gives users access directly to the applications that they need, when they need them. This significantly reduces the attack surface area that is available to adversaries.
- Access is restricted to users that meet a number of criteria, depending on their perceived riskiness:
  - Multi-factor authentication
  - Context checking. This means that the software asks questions like: What time is it for them? Where are they? What device are they using? If the user activity looks suspicious (strange time of day, location, device, type of request etc.) then they get assigned a high risk score and are required to meet additional security requirements. This process is repeated from time to time.

ZTNA is replacing VPNs in many cases; it is more appropriate for the modern Zero Trust architecture with widely distributed users accessing data and applications over the cloud.

vi. Secure Access Service Edge (SASE)

- SASE uses ZTNA as described above
- However it also delivers the following benefits:
  - Users access the service from their devices by interacting with their nearest 'point of presence' (PoP) in the cloud. That's basically a bunch of servers in London, New York, Singapore etc. that is managed by the provider.
  - Security is managed at the PoP, including
    - Advanced firewall
    - Data loss prevention
    - Cloud access security
  - Internet traffic is routed optimally over a private global network so that you get better performance and avoid circulation issues that are being faced by the public internet.
  - PoPs are usually located right next to the data centres that manage Azure, Google Cloud Platform and AWS, so that interaction with those services is faster and with lower latency.

vii. Online Intelligence/Threat intelligence

Online intelligence solutions scan the whole internet including the dark and deep web in order to help the organisation to manage the following risks:

- Attacks on the brand
- Fake, malicious websites

- Data and credential leaks
- Activity targeting executives
- Third party risks

Dark web forums and marketplaces also represent a useful source of threat intelligence regarding new exploits and vulnerabilities that have been discovered by the hacking community.

viii. Asset management

"Asset management is about the policies and processes that help the organisation to account for each of its assets throughout their respective lifecycles." (UK National Cyber Security Centre)

Asset management software searches out all the organisations IP-connected devices (all types of device including desktops, laptops, smartphones, BYOD and guest devices, routers, IoT devices etc etc. This enables the organisation to build a complete asset inventory.

A version of this type of software is designed specifically for industrial control systems in oil refineries, power stations, grid networks and similar.

Device detection and assessment is done using a range of passive and active monitoring techniques, and managed in a way that is not disruptive to the business-related activity and devices on the network, which can be very fragile due to legacy issues.

Those assets are then classified and continuously assessed in terms of configuration, software installation, version control and patching, along with many other attributes.

Rogue assets that should not be connected to the organisations systems are detected – even if they are pretending to be legitimate.

ix. Secure development tools

Secure development (which is to say building software applications so that security is baked in to them) is a relatively new focus area of information security.

Traditionally, programmers/developers did not concern themselves with security as – back in the day – they didn't even consider the possibility that their software would be targeted by attackers.

Subsequently, security teams started to look for vulnerabilities in code towards the end of testing or even at the production ('live') stage of the software development life cycle (SDLC). That means returning the software to the developers to fix problems – time consuming, expensive and inefficient.

Adversaries such as ransomware operators have become aware of how easy it can be to attack vulnerable applications, and also how fragile is the software supply chain via the open source components that make up the majority of code.

Nowadays, the trend is towards putting responsibility for software vulnerability management in the hands of the developers themselves, an approach called 'shift-left security' as security considerations are moved towards the beginning (the left) of the SDLC. A number of software solutions have been developed to assist engineers in the task of secure development and vulnerability testing:

- **Open source analysis (also known as Software Component Analysis or SCA)**

  Open source resources can be exploited relatively easily by attackers. For example, an attacker might create a fake open source component that has a very similar name to a popular, bona fide component. If a developer uses the fake one by mistake, then they may introduce a backdoor or similar malware into their application.

  SCA checks that the components are the intended ones, and that they are secure. It is also able to check the licensing conditions around the components, as in some cases there are some contractual obligations even with open source, and failure to comply with these might cause serious operational and legal problems.

- **Static and dynamic application security testing (SAST, DAST)**

  SAST checks through static code while it is being written by the developer and can integrate with nearly all developer tools (code editors etc.). It looks for vulnerabilities that the developer has unwittingly introduced into the code base, and then provides advice regarding remediation.

  Dynamic testing (DAST) monitors the code while it is actually running; also checking for potential vulnerabilities.

- **Container security**
  The current way of building large applications is based on modular microservices that run on Kubernetes containers. These containers are built up from open source container images that should be checked for secure configuration and the potential presence of malware.

x. SaaS security posture management (SSPM)

Organisations of any size use many SaaS applications nowadays, and they generally struggle to ensure that all of them are securely configured, potentially introducing serious risk into the organisation.

SSPM solutions connect to all the SaaS apps and provide 'single pane of glass' visibility into the status of all of them, flagging security risks. SSPM also generates an inventory of exactly what SaaS apps are being used and by whom.

xi. SIEM

These, like EDR/XDR, are sophisticated tools that require a lot of input from the user, and are aimed at fully staffed security teams that work for banks and other large organisations.

SIEM (Security Information and Event Management) gathers potentially relevant data from all kinds of disparate sources such as:

- Endpoints (desktops, laptops, mobile devices)
- Firewalls
- Intrusion detection system logs
- Active Directory and authentication logs
- User access and activity logs
- Web filters
- Threat intelligence sources
- IP geolocation data
- …

It then normalises all the data flows so that they can be analysed using correlation analysis, machine learning/AI, and other technical techniques in order to help analysts to spot anomalous and suspicious activity.

Note that SIEM puts a lot of responsibility for analysis in the hands of the analysts; it presents them with the data and they decide what to do. An EDR/XDR solution, on the other hand, makes the decisions – so it is a bit 'black box' for some people. It is arguably easier for an adversary to evade an EDR/XDR than a SIEM – but a SIEM is a lot more work…

xii. ICS Security

ICS security software monitors activity on industrial networks such as power stations, energy grid networks, refineries and other critical infrastructure.

The objective of the network monitoring is to detect anomalous and potentially malicious activity without disrupting sensitive ICS devices on the network.

Other functions that the software may offer include network segmentation and quarantining (to restrict the movement of an attacker) and authentication controls for users and applications that attempt to access the network.

5. Future information security risks (non-exhaustive, unfortunately!)

i. Artificial Intelligence and Information Security/Cybersecurity

There are two main areas to focus on here:

- **AI for attack and defence**
  Adversaries are already starting to use Large Language Models (LLMs) like ChatGPT to help them with phishing campaigns, and to develop advanced malware that can evade EDR solutions.

  Organisations that are concerned about the threat from AI-enhanced phishing and malware are recommended to use very advanced EDR/XDR and SIEM solutions, or MDR. They should also stay on top of threat intelligence sources that provide information about developments in this area.

- **Internal data breach risks**
  Many organisations have banned the use of AI/LLM applications in the workplace, as users have already started unwittingly to expose sensitive data via these apps. They are also worried about similar risks from applications that they use in their own apps that are LLM-powered, such as chatbots in web applications.

  There are specialised consultancies that can advise on this area, and one of the best ones is a partner of Kiowa Security.

ii. Post-Quantum Encryption

Practical quantum computing is likely to become available to certain countries within five to ten years, and in fact they may already be using it, for all we know.

One potential application of quantum computing is the breaking of several different cryptographic methods, including those that are used to encrypt/decrypt information that is transferred over the internet.

That will obviously be a problem when quantum computing becomes available to attackers, but in fact it is already a problem now. This is because adversaries are already gathering data that was encrypted using quantum-vulnerable algorithms, with a view to decrypting the data when the technology becomes available. Relevant sensitive data obviously include Official Secrets, but also personal data that don't change over a long period (tax data, social security numbers, addresses), medical data, trade secrets, crypto wallet keys and so on.

There is software that enables organisations to encrypt data in a way that is quantum-resistant, and Kiowa can advise regarding that.