CYBERSECURITY VS INFORMATION SECURITY – WHAT'S THE DIFFERENCE?

CYBERSECURITY VS INFORMATION SECURITY – WHAT'S THE DIFFERENCE?

Managing risk to avoid unnecessary cost and disruption is a key focus for any maturing organisation. As organisations grow and mature, they inevitably begin reviewing risks to their information and digital systems. In this space, cybersecurity and Information Security are two terms that are often used interchangeably, and while there is overlap, understanding the differing scopes and methods of each can equip an organisation with more tools to treat risk and ultimately help reduce their overall risk profile.

WHAT IS CYBERSECURITY?

Cybersecurity is a technical discipline that focuses on protecting, preventing damage to, and restoring electronic communications services and systems. In short, cybersecurity is the technical methods used to secure technical systems. Cybersecurity fits entirely in the realm of Information Technology.

Cybersecurity professionals focus on the secure configuration of cloud, network, and infrastructure, as well as the operation of systems designed to detect, prevent, contain and eradicate threats to the organisation's digital systems. Typically, cybersecurity looks at areas such as firewalls, anti-virus, web and spam filtering, and vulnerability management, amongst many more. The commonality between all these systems is that they are technology designed to protect other technology from technical threats.

WHAT IS INFORMATION SECURITY?

Information Security is a broad area, of which cybersecurity is only one element. Information security focuses on the confidentiality, integrity, and availability (CIA) of all information held by an organisation. It seeks to protect the confidentiality, integrity, and availability of any and all information stored by the organisation, regardless of the format, storage medium and type of threat. As well as cybersecurity, information security professionals are concerned with non-digital threats and non-digital information assets. As such, Information Security covers areas such as policies, procedures, roles, responsibilities, vendors, contracts and many more and cross all functions of an organisation.

For the purposes of Information Security, confidentiality, integrity, and availability are defined as:

- Confidentiality is the practice of ensuring that information is only available to those who are authorised to access it. In recent headlines, both Medibank and Optus failed to keep information they stored confidential when an attacker was able to gain unauthorised access, with devastating results to both organisations.

- Integrity is the practice of maintaining the accuracy and completeness of information stored by the organisation. This is achieved by ensuring information is not changed without reason and authorisation and is not tampered with. For example, if an attacker were able to change the balance of their own bank account, they would have breached the integrity of the bank's information.

- Availability is the practice of ensuring data is available to those authorised to access it. When attacks encrypt data or make systems unavailable, then the accessibility of information has been compromised.

WHAT'S THE DIFFERENCE?

Cybersecurity can best be viewed as a sub-activity of Information Security. While both cybersecurity and information security are concerned with protecting digital information, Information Security also broadens its scope to include physical data, such as printed files and documents, as well as intellectual assets, such as the knowledge of employees.
Information Security also looks at a broader scope of threats to the confidentiality, integrity and availability of the information it seeks to protect. Information Security has a heavier focus on governance, risk and compliance activities and will seek to identify and treat risks coming from weaknesses in such areas as corporate policies, contracts and non-disclosure agreements, employee screening & employment terms, intellectual property rights, privacy, roles and responsibilities, segregation of duties and many more.

WHAT DOES INFORMATION SECURITY GIVE AN ORGANISATION THAT CYBERSECURITY DOES NOT?

Cybersecurity is an important first step for small organisations. Without foundational cybersecurity, organisations face significant risks across all of their digital systems. However, as organisations grow, the risks they face from non-digital attack vectors grow, and this is where information security can build upon cybersecurity foundations.

In fact, in the latest 2022 publication of ISO27001, the international standard for Information Security, only 36% of the security controls it contains are in the cybersecurity realm. The other controls fall under the categories Physical (15%), People (9%) and Organisational (40%), representing the broader scope of information security.

Some of the key areas covered by Information Security but not cybersecurity, according to the ISO27001 standard, are:

ORGANISATIONAL CONTROLS:

Organisational controls seek to secure information through the way an organisation operates and its policies, processes and procedures. Some of the key areas covered within the organisational domain are:

Information Security Policies: This area seeks to ensure that the organisation has appropriate policies in place to govern the collection, transfer and storage of information. It ensures that policies, which govern how the organisation operates across all areas, are aligned to and appropriately reduce the risks the organisation faces to the confidentiality, integrity and availability of information assets.

By implementing clear policies, organisations ensure that the security of information is considered as part of all operations by both management and employees.

Organisation of Information Security: This area ensures that roles and responsibilities for information security are considered by management and assigned to relevant individuals. This drives accountability for an organisation's holistic security posture, and ensures specific areas are not forgotten about.

Ownership and accountability for the security of information also leads to a continual improvement in the space, and ongoing consideration and reduction of associated risks.

Supplier relationships & contracts: While cybersecurity focuses on protecting an organisation's own systems, information security extends its scope to ensure that organisation information is secure even after it has been shared with an authorised third party. Modern organisations make use of external services which require their information in many areas, everything from emails on Microsoft's cloud to financial data on Xero's cloud. Ensuring that these types of suppliers and partners are protecting an organisation's data is becoming more and more important in the modern business ecosystem.

Privacy and protection of PII: This area evaluates the legal, regulatory and contractual requirements of an organisation related to the protection of Personally Identifiable Information (PII). Looking beyond just the technical defences an organisation implements to protect the personal information is gathers and stores, this control seeks to ensure the organisation is aware of the private information it holds, complies with relevant legal considerations and appoints relevant responsibilities, such as a data privacy officer. It also asks abstract questions to help reduce the organsations risk, such as do we really need to store this data?

PEOPLE CONTROLS:

One of the major risks modern organisations face to the security of their information is through their people. All organisations have valuable information assets such as tools, templates, cost calculators or pricing books which give them an advantage over their competitors. However, in order to operate, people need access to this sensitive information, and people often lack guidance or awareness of their responsibilities to keep information secure. This can lead to the accidental sharing of confidential information. Its also becoming increasingly common for employees to frequently change employers throughout their careers.

People controls seek to ensure information security is considered and communicated through initial employee screening and onboarding, through the terms and conditions of their employment, that appropriate confidentiality or non-disclosure agreements are in place, and that information security obligations persist after employment to protect the organisation from accidental, unaware or intention risks to information security that employees may not be aware they are creating.

Two of the key goals of People controls are to ensure that information is handled securely while employees are working, and to protect information assets from being shared with competitors when an employee leaves the organisation.

PHYSICAL CONTROLS

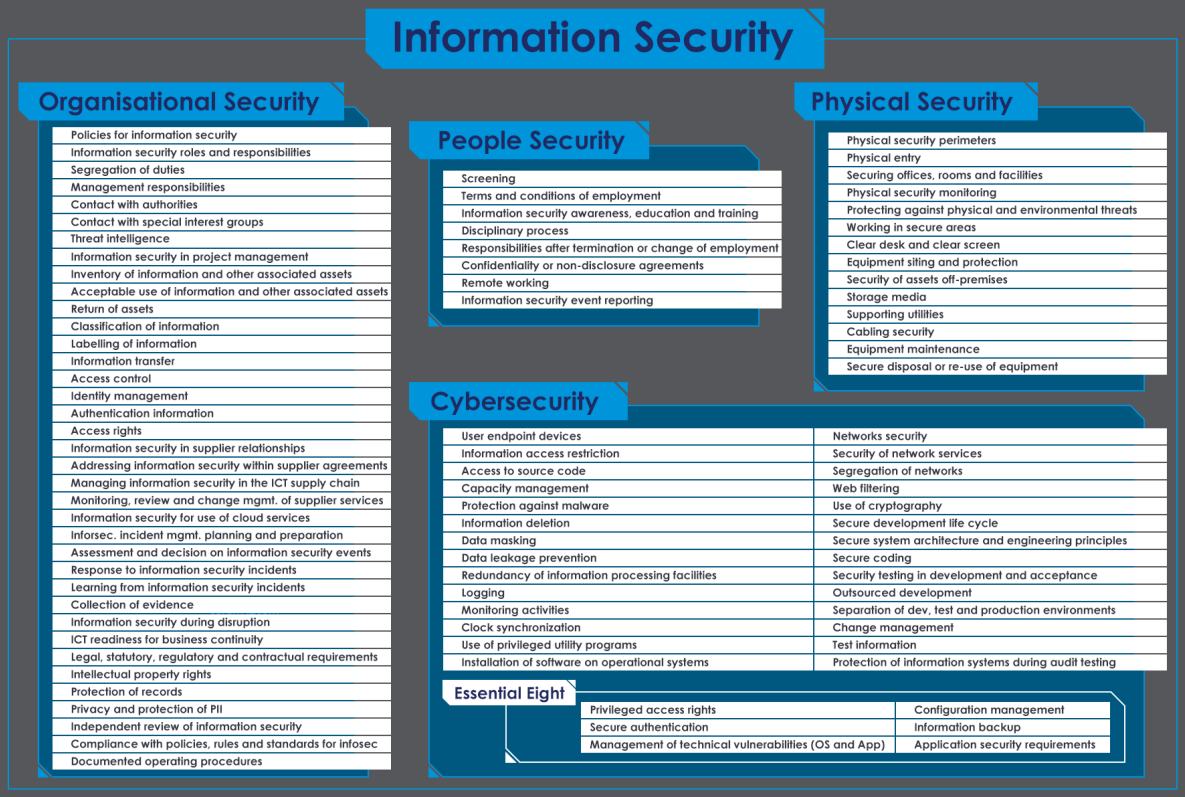
Information Security also expands its scope to the physical security of information. Whether that information resides in digital format on computers, or in physical documents in desks and filing cabinets, information security seeks to ensure computer rooms, offices and working spaces, including home offices, are secure to prevent data breaches. Controls such as physical perimeters, clear desk and screens and secure disposal/reuse of assets help protect an organisation from both accidental and intentional data breaches.

CONCLUSION

Cybersecurity is a subcategory of Information Security and focuses on the technical methods used to protect digital systems from cyber threats. Cybersecurity is entirely in the realm of IT professionals. Information Security, however, is a much broader topic. Information Security seeks to examine an organisation's operations through its policies and procedures, as well as how it deals with the security of information in contracts, relationships, roles and responsibilities.

While led and advised by Information Security professionals, it spans all areas of an organisation and seeks to mitigate digital and non-digital threats to an organisation's information.

Ultimately, in modern organisations, competitive advantage is increasingly being achieved through information assets. Be it client databases, commercially sensitive documents, or internally developed costing and quotation models. Information security provides a much broader lens to identify and mitigate threats to these assets and maintain those competitive advantages.



advance

CONTACT INFO

+61 8 8238 6500

sales@advance.net.au

www.linkedin.com/company/advance-business-consulting/

www.advance.net.au