CCC Item III: Security Cheatsheet

Thomas Boxall
up2108121@myport.ac.uk

May 2023

1 Definitions

Information Security is the preservation of confidentiality, integrity and availability of information. There is a balance to be found between the three, as often when you change one the others will change negatively.
Confidentiality is the property of information which means it is not disclosed to unauthorised individuals, entities or processes.
Integrity is the property of safeguarding the accuracy and completeness of assets.
Availability is the property of being accessible and usable upon demand by an authorised entity.
Assets are anything of value to the organisation, its business operations, and its continuity.
Threats are potential causes of incidents that may result in harm to a system or organisation (can be internal or external).
Vulnerabilities are weaknesses of assets or groups of assets that can be exploited by *threats*.
Impact is the result of an information security incident which has been caused by a threat and affects assets. (e.g. monetary loss, fines, loss of reputation)
Risk Management is the process organisations go through to identify, assess and control risks.
Object of an attack is the entity which is being attacked, the target.
Subject of an attack is the entity carrying out the attack against the target. The subject attacks the object.

2 Assets

Primary Assets are information or business procedures. These are the most valuable things to the organisation.
Supporting Assets are other assets who, if compromised, could adversely impact primary assets.

2.1 Primary Assets

Information assets are typically of the highest value to an organisation. Especially the case for *business critical information* (without which, business could not operate), *personal information* (data of employees and customers, must be protected in accordance with the law), *strategic information* (gives the business an advantage in the market), and *high-cost information* (gathering, processing, storage, transmission is expensive - if lost then business has to spend lots of money again).
Business Processes are processes which: contain secret processes; involve proprietary technology; if modified can affect the outcome of the organisation's mission; are necessary for the organisation to comply with contractual, legal or regulatory requirements. If a business fails to document or protect these procedures significant adverse effects can be had, often this will come to light when an employee is off sick or on holiday, or leaves the company all together and it is discovered that the processes they oversaw are not sufficiently documented.

2.2 Supporting Assets

Hardware Assets are the physically technology which is used to: house and execute the software; store and carry the data; or provide the interface for data entry/ removal from the system. Hardware assets cover most physical technology (e.g. computer, laptop, keyboards). Hardware devices should also have adequate physical protection.
Software covers all applications, operating systems and assorted command utilities. Development of software is often under-resourced which leads to security being an afterthought not implemented throughout, this is bad and ideally security would be implemented throughout the software development cycle.
Networks are responsible for the effective transmission of information between interconnected computing devices. They are also a very good vector for attacks. The likelyhood of an attack succeeding can be reduced by implementing policies and technical responses as well as examining ports and packets at the perimeter of the network to ensure only the data which is necessary for business function is being exchanged. The later is done using a firewall. The internal network should also be protected through segregation of critical systems, access controls and monitoring software.
Personnel are the people who are interacting with the information systems and are the subject of numerous vulnerabilities. Anyone interacting with an information system should be given appropriate training. Organisations should also develop a comprehensive set of policies which should be written using plain business terminology with minimal use of technical jargon. The effectiveness and awareness of information security should be monitored.

3 Information Security Governance

Information Security Governance is how organisations control, direct and communicate their cyber risk management activities. This will include a collection of policies which must be continually reviewed and revised to keep up-to-date with the business needs and continually changing threats/ vulnerabilities.
Policies are a principle or rule to guide decisions and achieve rational outcomes.
Procedures are a list of steps that constitute instructions for performing some action or accomplishing some task.
Standards are detailed statements which quantify what must be done to comply with policies.
Guidelines are a set of recommended actions to assist in complying with policies.
SETA *Security Education, Training and Awareness* is a programme that helps employees do their jobs securely.

4 Identification & Authentication

Authentication of claimed identities is the first line of defence for the system and safeguards against unauthorised use.
Passwords are the most common means of authentication, conceptually simple however they are weak: badly selected, written down, infrequently or never changed, reused across multiple systems, forgotten, shared.
Users must be able to identify user-specific access controls and be held individually accountable for their actions.

4.1 Passwords

Lots of vulnerabilities with use of passwords including: easy to select a bad one, get written down, infrequently or never changed, same password used for multiple systems, only needed at the start of a session.
Defence against password guessing is traditionally to lock the user out after a number of failed attempts is a form of *denial of service*.

5 Access Control

Identity is the properties of an individual or resource that can be used to identify uniquely one individual or resource.
Authentication is the process of ensuring that the identity of a subject or resource is the one claimed.
Authorisation is the process of checking the authentication of an individual or resource to establish their authorised use of, or access to information or other assets.
Accounting ensures that user activities can be tracked back to them
Auditing is the process of either a formal or informal review of actions, processes, policies and procedures
Compliance is working in accordance with the actions, processes, policies and procedures laid down.

5.1 Access Control Policies

Discretionary Access Control Policy (DAC) - controls access based on identity of individuals. Each access controlled object must be set individually for each user.

Access Control Matrix permissions are shown as a matrix with a subject having a single entry for each object containing all their permissions.

Access Control List (ACL) stores all the permissions for a single object in a 'linked-list' style structure, with each index representing a subject's access levels.

Capability List stores all the access rights for a single subject in a 'linked-list' style structure, with each index representing a different object that subject has access to.

Mandatory Access Control Policy (MAC) - controls access based upon security labels. Users are assigned under a clearance level which defines what they have access to. Labels may include: top secret, secret, classified, unclassified. A number of models are available for access control.

Bell LaPadula (BLP) Model provides subject with no access to anything above their level but read access to everything below.

Biba Integrity Model provides a "no write up, no read down" model

Clark-Wilson Integrity Model provides a model where no changes may be made by unauthorised subjects, no unauthorised changes can be made by authorised subjects, and maintains internal & external consistency.

Graham-Denning Access Control Model uses objects, subjects and rights.

Brewer-Nash Model allows subjects to only access one of two conflicting sets of data, preventing conflicts of interest.

Role-Based Access Control Policy (RBAC) - controls access based on roles. Users are assigned to one or many roles. Roles come with permissions. Users inherit permissions of the role.
Attribute-Based Access Control Policy (ABAC) - controls access based on attributes of users. It uses various attributes of the user including their environment and information assets to determine permissions.

6 Authentication

Factors of Authentication are mechanisms by which an individual or resource can be authenticated. The three common factors are: *something the supplicant knows* (PIN number, password), *something the supplicant has* (security token, bank card), and *something the supplicant is* (fingerprint, retina/ iris scan).
Strong Authentication is a procedure based on the use of two or more *different* factors. The factors used should be mutually independent (which means if one is compromised, the other isn't).

6.1 Biometrics

Biometrics is the use of a body measurement (e.g. fingerprint) as a factor of authentication.
False Rejection Rate (FRR) is the percentage of identification instances in which authorised users are denied access (Type I error)
False Accept Rate (FAR) is the percentage of identification instances in which unauthorised users are allowed access (Type II error)
Crossover Error Rate (CER) is the level at which the number of false rejections equals the false acceptances
Requirements of a biometric system: universality, distinctiveness, persistence, collectability, performance, acceptability, circumvention.

7 Cryptography

Cryptography is a way of turning plaintext into cyphertext (which can later be turned back into plaintext).
Encryption is the process of altering the plaintext so that it becomes unreadable to the normal human.
Decryption is the process of altering the cyphertext so that it returns to plaintext.
Cryptographic Algorithm is the algorithm used to encrypt/ decrypt the data. Modern algorithms should be: large enough key to resist brute force search; resistant to frequency analysis; setup so that a small change in the plaintext results in a large change in the ciphertext; and that the security depends on the secrecy of the key & not on the secrecy of the algorithm used.

7.1 Cryptographic Algorithms

Symmetric is where encryption and decryption both use the same key. This results in both the sender and receiver needing the same key.
Asymmetric is where the encryption and decryption use different keys. This is complex so is often used to encrypt the symmetric secret key which has been used for encryption for the main data transmission.
Caesar Cipher is a simple cipher where letters are substituted for other letters in a circular motion.
RSA is a asymmetric cryptographic algorithm which uses prime numbers and maths to encrypt each character in the transmission.

8 Risk Management

Risk Management the process of identifying and reviewing risks so that they can be minimised/ removed.
Risk has three elements: threat, vulnerability and impact. The higher likelihood and impact of a risk, the higher risk the activity is.
Risk Assessment Steps identify risks, analyse risks, treat risks, monitor & review.
Qualitative Risk Analysis uses a scale of attributes to determine the magnitude of the consequences/ likelihood. Can be used as initial screening to identify risks requiring detailed analysis.
Quantitative Risk Analysis uses a sale of numerical values for consequences/ likelihood values. Typically these numbers are derived from historical incidents.
Critical Appraisal of Risk Methods and Frameworks was produced by the NCSC so risks can be better understood and approaches available can be supported. Context is important when using a framework.

8.1 Risk Treatment Options

Retain / Accept where an organisation may tolerate (but not ignore) the risk.
Avoid / Terminate where an organisation may decide not to do the thing that incurs risk.

Share / Transfer where the risk is transferred or shared via an insurance policy or third party.
Modify / Reduce where controls are adopted to lower the current levels of risk.

9 Common Software Errors

Software is highly-prone to causing security compromises. This is mostly due to the fact that software development is under-resourced which leads to security being added as an afterthought.
Web Applications may have attack vectors however finding the path from threat agents through attack vectors, security weaknesses, security controls, technical impact, to business impact can be very difficult.
Security Requirements Specification should be part of the overall statement of requirements document from which the design is generated.
Security doesn't just mean prevent improper access and misuse, it also means defensive programming (to make sure only valid and accurate data is processed by the system); proper functional testing (to ensure it behaves as expected); methods to back up secure data against loss or damage; and compliance with any legal and regulatory requirements.

10 Typical Web Errors

Cross Site Scripting (XSS) is where the input on a webpage is not neutralised correctly.
Reflected XSS is where the victim's browser executes code based off on an input which has been made in the browser.
Stores XSS is where the app stores the bad data in a database which is later read into the app and included in dynamic content.
SQL Injection is where a piece of software doesn't properly sanitise an input which is directly fed into a SQL query. Malicious code can be inserted which can display content from the database.

11 Secure Development & Deployment

All developers are responsible for security during development. It is important to secure the code, build & deployment pipeline and continually test the security.
It is generally regarded as good practice to fully isolate the development and production environments as well as treating the development environment as if it is compromised.
Change Control should be strict for production software. At least two people should be involved in pushing code, preferably one writes it and another approves it.
Patching of software should be done as soon as bugs are found. Before releasing into a production environment, patches should be tested in development environments.

12 Accreditation and Certification

Accreditation is formal recognition by an independent body (the accreditation body) that a certificate body operates according to international standard.
Certification is provision by an independent body that the product, system or service in question meets specific requirement.