ASPIRENET LTD

Risk Management

Risk Assessment Toolkit

Information

Document ID	ASP-RA-Toolkit
Version	1.0
Date of Version	21st July 2020
Author	Kenny McLean
Role	Consultant
Classification	Public
Next Review Date	21st July 2021

Version History

Version Number	Date	Author	Description of Change
0.1	27th June '20	Kenny McLean	Initial Draft
1.0	21st July '20	Kenny McLean	Published

Abbreviations & Acronyms

Abbreviation / Acronym	Description
API	Application Programming Interface
CSRF	Cross Site Request Forgery
DDos	Distributed Denial of Service
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transfer Protocol
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PNT	Positioning, Navigation & Timing
SQL	Structured Query Language
XML	Extensible Mark-up Language
XML EE	Extensible Mark-up Language External Entities
XSS	Cross Site Scripting

Contents

1. Purpose

The purpose of this document is to give the reader a standard list of those threat sources, actors, and vulnerabilities as a baseline for use during a risk assessment.

2. Scope

This document will cover those areas applicable when carrying out a risk assessment and also give the reader an example threat scenario which they can then use as guidance when carrying out a risk assessment.

3. Introduction

This catalogue of Threats is to be used as guidance only and is not a definitive list. As new threats emerge and new technologies evolve, these should be added to the relevant table in order to assist users in carrying out ongoing risk assessments, or the re-evaluation of current risks against the identified asset (whether that's information, hardware, software etc.)

Please note that some Threat Actors may also be applicable to Threat Source. Typically, a Threat Source is usually a person or organisation who wishes to cause a breach and ultimately benefit from that breach. A Threat Source may require a Threat Actor to carry out this breach, i.e. an inside employee who has been blackmailed by an organised gang to carry out the breach. However, the Threat Source may also be the Threat Actor, for example, a dissatisfied employee.

The impacts are a result of a compromise to one or more of the CIA triad (Confidentiality, Integrity & Availability). There is however a fourth consideration, that being Non-repudiation.

4. Threat Scenario

A Threat Source motivates a Threat Actor to carry out a Threat Method/Event via exploiting a vulnerability through capability and opportunity. A successful exploitation of a vulnerability which realises a threat method/event will result in a one or more of the possible impacts.

4.1. Threat Scenario Example

A Commercial Competitor (Threat Source) bribes (Motivation) a Supplier Employee (Threat Actor) to carry out Information Theft (Threat Method/Event) due to the Lack of security controls for suppliers/service providers (Vulnerability, Capability & Opportunity). Successful exploitation of this will result in Reputational and possible Financial and individual impacts (Impacts).

5. Threat Sources

Threat Source	Description
Criminal Gang	A criminal group who have the motivation to carry out a cyber-attack for financial gain
Foreign State/Government	Foreign state government or security services who may wish to carry out a cyber-attack in order to cause political instability, theft of trade secrets, theft of national secrets etc.
Political Activist Group	A group of individuals with the same political ideology and who may wish to cause criminal damage or theft.
Individual Criminal	An individual who will carry out criminal activity for their own personal financial gain.
Commercial Competitor	An organisation or business who are in direct competition and who may wish to carry out industrial espionage against your business.
Terrorist Group	A group, or an individual acting on behalf of a terrorist group, who wish to cause harm or destruction to the public or national infrastructure, due to their political, religious, or ideological beliefs.
Dissatisfied employee (insider threat)	A current or previous employee who has a grudge against the business or individuals within the business, and who is intent on causing financial or reputational damage
Employee	A standard employee with standard user access who may, or may not, act maliciously
Malicious Attacker	An individual who has the ability and means to carry out a cyber-attack on the organisation for financial gain
Environmental	Severe weather or damage/fault to utility services resulting in a flood or fire
Supplier	An organisation within a supply chain that may introduce unwanted vulnerabilities either unintentionally or intentionally

6. Threat Actors

Threat Actor	Description
Privileged User (passive)	This employee requires elevated system privileges in order to carry out their work within the business. Typically, a network or system administrator
Standard User (passive)	A standard employee with only standard restricted access to the network and systems
Dissatisfied employee (insider threat - aggressive)	An employee who has a grudge against the business as a result of multiple possible reasons such as non-recognition, being disciplined, disagreement with superiors etc.
Opportunistic Criminal	These criminals act when an opportunity arises that is unexpected, such as an unlocked car, mobile phone left behind in a café etc.
Organised Criminal	Usually gangs who work together in order to create a distraction in order to carry out their theft. Or cybercriminal gangs who work together for large financial gains
Terrorist	Groups or lone individuals who have the ability to cause destruction to life or national infrastructure
Physical Intruder	A criminal who will break an entry to a building in order to carry out criminal activity
Supplier Employee (passive or aggressive)	A company or organisation who supplies equipment or information, which the business relies upon in order to carry out a business function
Service Provider Employee (passive or aggressive)	A company or organisation who provides services to the business in order to assist the business in carrying out its day-to-day operations
Hacktivist	An individual who gains unauthorized access to computer files or networks in order to further social or political ends.
Script Kiddie	An individual who uses existing computer scripts or codes to hack into computers or networks, who lacks the expertise to write their own code or exploits.
Malicious Attacker	An individual who has the technical ability and expertise to create or write code, in order to gain unauthorised access into computers or networks.
Adversary (State Sponsored Attacker)	An individual who has been employed by a government agency in order to gain unauthorised access. They may be within physical or geographical range of protected assets. They will more than likely have the financial and technical support to carry out a range of physical, electronic & logical attacks
Business Competitor	An individual or group who has been employed by a competitor in order to carry out industrial espionage

7. Threat Method

Threat Method	Description
Malicious intrusion	Unauthorised access to the infrastructure via multiple methods, with the intention to carry out criminal activity (by use of application bugs or buffer overflows for example)
Distributed Denial of Service (DDoS)	DDoS is a method which floods systems with network traffic in order to deny users/customers access to the requested resources
Network Scanning	A method of reconnaissance carried out by someone trying to determine what possible vulnerabilities are open for exploitation
Man-in-the-middle	When a malicious individual succeeds in placing themselves in the communication path between a client and another device, usually a server, in order to eavesdrop
Session Hijacking	Session hijacking is when an individual’s authentication cookie is copied or stolen and then replayed back to the authenticated server. E.g. through XSS, CSRF
Website defacement	When someone successfully access the management interface of a website, and/or, successfully exploits a known vulnerability of the software running on the website, in order to deface a website.
Information theft	Theft of information by someone who has either successfully accessed the network, or by an opportunistic means
Phishing	Socially engineered emails sent to users in order to gain financial information, or to gain access to a system
Social Engineering	A means by which malicious individuals 'trick' users into revealing information, or granting physical access, which will assist the criminal in carrying out their crime.
Physical Theft	Theft of assets left unattended or theft of assets from premises
Unauthorised Physical Access	Unauthorised physical access can be gained by Tailgating, social engineering, lack of identity checks etc. and may lead to a number of outcomes such as theft, arson, vandalism, malware injection, insertion of rouge devices etc.
Malware	The use of malware is the main method used for malicious individuals to gain unauthorised access to corporate systems, computers etc.
Loss of an asset	Accidental loss of an asset that may contain sensitive information
Unauthorised logical Access	Access gained through usual access methods which give a user access to systems, data or information that they should not have permission to (through use of stolen credentials for example)
Authorised Access	Users have the ability to abuse the access rights they have been granted in order to extract information or data for personal reasons
PNT Attack	Positioning, Navigation & Timing attacks may be used to disrupt data traffic or give false location information to/from physical assets.

Threat Method	Description
Data Manipulation	An attacker may be able to manipulate the integrity of data whereby false information is disseminated to users/customers/consumers

8. Typical Vulnerabilities

Vulnerability	Description
Poorly written policies	Poorly written policies and/or supporting procedures lead to lack of guidance for employees and enforcement of the business needs in regard to security
Leavers/movers access rights not being changed	Not revoking access rights when an individual changes role, or leaves the organisation, leaves authorised access rights available to someone who no longer requires those rights
weak passwords	Weak passwords are easily cracked with the use of brute force tools or password dictionaries
Default accounts being left activated with default passwords	When administrators do not disable default accounts, or change the default password for those accounts, it gives a malicious individual easy access into systems.
No clear desk/screen enforcement	If a clear desk/clear screen is not enforced, employees may leave sensitive information on the desk or showing on their screen when they are absent from their desk.
Failure to segment networks	Segmentation of networks allows for the separation of data traffic which are classified at different levels of sensitivity. This also allows for the denial of access to information from those who sit in different business functions
Failure to implement secure mobile security	Implementation of mobile security grants administrators the mechanism required to enforce security controls on devices which are frequently out of the office environment and at a higher risk of loss

Vulnerability	Description
Failure to test new software prior to deployment	Failure to test software or systems prior to deployment in a live production environment will inevitably fail to highlight any security flaws that are present, and therefore, open the availability of them to the public/users
Failure to implement least privileges	Users only require the access rights they require to carry out their role. By not following the method of least privilege, users will be granted access to systems, information, software that may be used maliciously if intended
Failure to implement segregation or separation of duties	Separation/segregation of duties should be implemented for key processes, or processes where sensitive information is handled, to ensure that no 'one' person is responsible for that process, as this could lead to abuse of position.
No media disposal procedure	Without a media disposal procedure, there is a risk that sensitive data may be unintentionally passed on to other individuals who should not have access to that data.
No change management procedure	Without a change management procedure, there is no auditable record of changes in addition to the absence of captured testing or risk assessment for the change required.
No anti-virus deployed	End points that do not have any anti-virus involved are at greater risk of being infected and ultimately breached/compromised by malware. These devices would become 'jump' points for breaches into a network
No patch management procedure	Without a patch management procedure, security patches for OS' or installed software will be missed, exposing the device without the patch to possible exploitation of known vulnerabilities.
Weak access controls	Weak access controls lead to users bypassing those controls, thereby allowing them to access information/data/systems that they would ordinarily not have access to.

Vulnerability	Description
No backup policy	Without a backup policy, the organisation leaves itself open to the critical risk of data loss and productivity due to either environmental, technical, or malicious causes.
Weak encryption methods	Weak encryption methods allow those with malicious intent to easily decipher captured encrypted data
No Supply Chain Assurance	Without supply chain governance or assurance, a business could leave itself open to multiple vulnerabilities such as the introduction of malicious code, lack of hardware/software support, unauthorised access etc.
No data loss protection	Data Loss Protection prevents and identifies the extraction attempt, of information which the business has classified as sensitive
No Security awareness training for employees	A good security awareness programme educates the organisations employees on how to identify, and respond to, security risks whether it be social engineering, technical issues, or systems development.
Lack of Physical protection	Improper, or lack of, physical security controls will fail to identify intrusions to buildings, or secure areas or tampering with access points or equipment externally located.
Lack of technical security devices	Without the required security devices implemented, there is a high risk that malicious activity will be missed, resulting in a breach or loss of data.
Lack of security controls for suppliers/service providers	Without the correct controls put in place between the business and supplier/service provider, there is a risk that 3rd parties may have access to information/data/systems that they should not have access to. Additionally, they may not have the security controls in place within their environment that the business deems sufficient for processing data which has been given to the 3rd party.

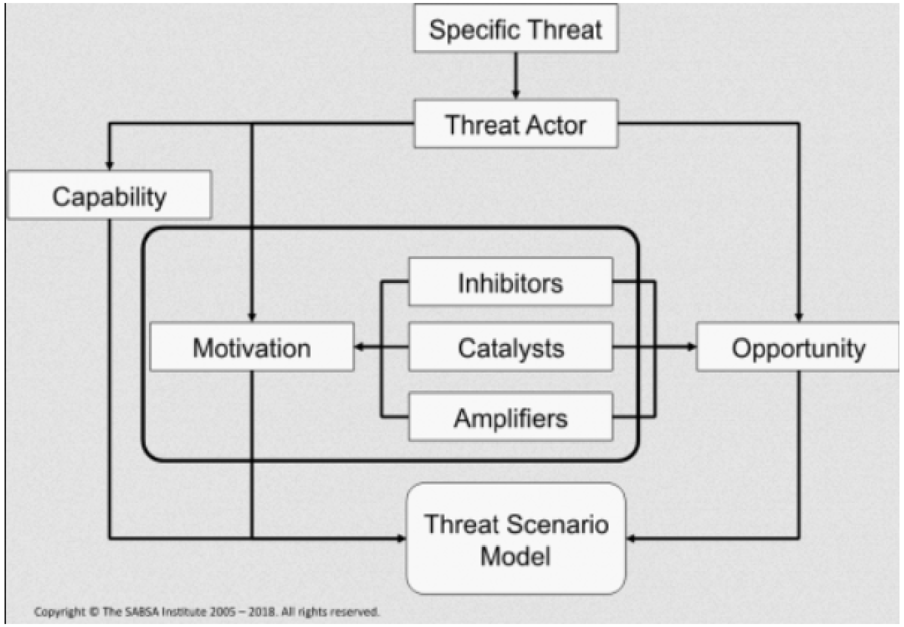
Vulnerability	Description
No incident response plan	A good incident response plan allows the business to identify, respond, contain, eradicate & recover in an organised well-rehearsed manner. Without this, breaches can go undetected with the possibility that remanence of the exploitation may remain after detection, allowing further breaches. Without preparation, individuals may not know their role in the event an incident occurs.
Lack or no redundancy/failover mechanisms	Without the implementation of redundancy or failover mechanisms, the organisation leaves itself open to a compromise which could take the business offline for a period that may result in heavy financial losses.
No DDoS Protection	Having no DDoS protection will leave your website and/or services open to a compromise of availability and potentially financial & operational Loss
Lack of environmental controls	Without the implementation, or lack of, environmental controls, there is a high risk that in the event of an environmental event (e.g. fire, flood, adverse weather) the businesses systems will be taken offline and result in heavy financial losses for replacement systems and loss of production.
Human Error	Accidental loss of information can occur when data is handled incorrectly or miss-configuration of systems can cause and accidental denial of service or unwanted information exposure. These are usually due to Human error.
Lack of or no background checks of employees	A lack of or no background checks of employees could result in the employment of an individual who is susceptible to blackmail or who does not meet the security vetting checks required to carry out their assigned role.

9. OWASP Top 10 Web Application Vulnerabilities

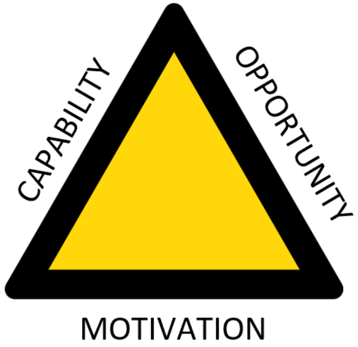
Vulnerability	Description
Injection Attack	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
Broken Authentication	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
Sensitive Data Exposure	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
XML External Entities (XEE)	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
Broken Access Control	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.
System/Security Misconfiguration	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.
Cross-Site Scripting (XSS)	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

Vulnerability	Description
Insecure Deserialization	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.
Using Components with Known Vulnerabilities	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.
Insufficient Logging & Monitoring	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

10. Threat Scenario Framework



11. Threat Triad



12. Motivational Influencers

Motivation & Opportunity Influencers		
Inhibitors	Catalysts	Amplifiers
Fear of Capture	External Events that trigger a response	Peer Pressure, blackmail
Fear of Failure	Changes in personnal circumstances creating a 'need'	Fame
Insufficient Access Limiting Opportunity	Step changes in level of access increasing the opportunity	Easy access providing high level of opportunity
High Level of Technical Difficulty	Step changes in level of difficulty through new technologies and tools	Ease of execution because of low level technical difficulty
High cost of participation	Step changes in level of cost	Low cost of participation
Sensitivity to adverse public opinion	Dramatic changes in public opinion and cultural values	Belief in sympathetic public opinion

13. Possible Impacts

Possible Impacts	
Impact	Description
Operational Impact	Loss of information, Reduced productivity, Loss of customers, Loss/theft of equipment etc.
Financial Impact	Increase in insurance premiums, hardware/software replacement costs, cancellation of contracts, legal penalties etc.
Legal & Regulatory	Fines, contractual penalties, fraudulent losses
Reputational	Loss of confidence, user/customer concerns, industry image, competitors taking advantage
Individual	Stress to compromised individuals, employee low morale