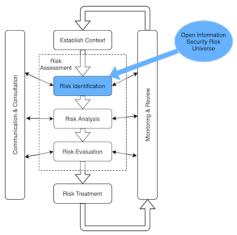
Open Information Security Risk Universe

1 Table of Contents

2 Introduction

A Risk Universe provides a comprehensive view of the possible risks we face. This view is designed to aid in categorisation but also to act as a check on the scope of our risk identification exercises to ensure we don't miss risks that then take us by surprise when they occur.

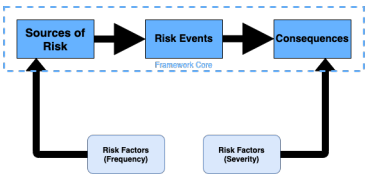


The goal of the Open Information Security Risk Universe (OISRU) is to provide a model and method independent framework for expressing and categorising security risk.

This framework should be complementary to the Basel II operational risk event types, recognising that information security risk permeates operational risk.

2.1 Overview of the Risk Universe

The Open Information Security Risk Universe comprises, at it's core, Sources of Risk Events, Risk Events and Consequences of Risk Events. These are supplemented by Risk Factors that drive the Frequency or Severity of the Risks.



2.2 Contributors

The following people have contributed to this document * Phil Huggins * Paul De Luca * Robin Oldham

2.3 License

3 Supporting Approaches

3.1 Risk Statements

It's key to understand that a risk event alone is not a risk, at it's most simple it is a risk event and a consequence.

However it is likely as we develop our risk sceanrios that they will consist of the combination or one or more sources, one or more risk events and one or more consequences.

While the description of the risk scenario under consideration can be tailored to use language appropriate to the organisation in scope and the stakeholders or experts that must consider it the undelying statement of the risk that scenario represents can, and should, be standardised using the Open Information Security Risk Universe.

At it's simplest a risk scenario can be truned into a risk statement using:

There is a risk that <**event**> occurs leading to <**outcome**> that causes <**consequence**>.

An example of a minimal risk structured as above is:

"*There is a risk that financially sensitive data is accidentally emailed to an external recipient leading to an information breach which results in regulatory fines.*"

Adding a source to the risk can aid in explaining the sceanrio such as:

There is a risk that <**source**> causes <**event**> to occur leading to <**outcome**> that causes <**consequence**>.

An example of a minimal risk structured as above including a source is:

"*There is a risk that a member of staff accidentally emails financially sensitive data to an external recipient leading to a data breach which results in regulatory enforcement.*"

By ensuring that every risk scenario is formally stated in this way it allows comparison between scenarios as well as identifying what coverage of the OSIRU is currently being considered by the organisation and whether that is appropriate.

By adding the significantly correlated risk factors it is possible to start discussing control measures to limit the risk exposure.

A risk statement including risk factors and controls might include the additional statement:

"*The financially sensitive data is market sensitive information before the annual report is published, but the data leakage control is configured to look for financial reports and to prevent their external transmission, and the Outlook autocomplete function is disabled for the period of the production of the annual report.*"

4 Sources of Risk

These are the various actors that cause a risk event to occur. They have different motivations and capabilities.

4.1 Internal Sources

Internal sources are actors that are within the trust and control boundary of the organisation.

- Disgruntled
- Accidental
- Ineffective
- Criminal
- Coerced

4.2 External Sources

External sources are actors that exist outside the trust and control boundary of the organisation.

- Criminals
- Hacktivists
- Compromised suppliers
- State-sponsored
- Competitor
- Press
- Researcher
- Regulator

4.3 Characteristics

It can be useful to consider characteristics of each source when analysing risks, the following charcteristics can be useful to consider:

- **Goals** (Curiosity, Personal Fame, Personal Gain, National Interests, Revenge, etc)
- **Skills** (No technical skills, End user, Power user, Developer, Researcher)
- **Knowledge** (External to organisation, Ex-Organisation insider, Organisation partner, Customer, Employee, Other insider)
- **Opportunity** (Connected to Internet, Physically nearby, Access to connected partner, Access to organisation, Access to specific network / system)
- **Deterability** (Unconcerned criminal, Careful criminal, Careless law-abiding, Careful law-abiding)

5 Frequency Risk Factors

Risk Factors are estimable values that are correlational but may not be directly causal to the risk. An increase in a risk factor may not directly drive an increase in the risk but is indicative of increase of the risk and will be useful for better informing expert estimation fo the overall risk. A positively correlated risk factor increases as the risk increases.

Frequency risk factors are relevant to the estimation of the frequency by which a risk is expected to occur.

5.1 External Frequency Risk Factors

External Frequency Risk Factors are risk factors that are outside of your scope of control that may affect frequency of the risks you manage.

These are stated as questions to ask yourself or your organisation. The ability to estimate or measure these risk factors will vary between organisations.

- Will an attacker attack us?
- Will an attacker attack our supplier/s?
- Does an attacker have the ability to attack us?
- Are there any hacking campaigns targeting our sector?
- Are there any hacking campaigns targeting our geography?
- Are the tools / knowledge required to attack us readily available?
- Has there been any change in staff stressors (financial, emotional, medical, etc)?
- Have any of the suppliers we trust been compromised?
- How easy is it to impersonate our suppliers staff or company?
- How aware of security are our suplliers staff?
- How quickly do our suppliers patch their systems?
- Do our suppliers have effective governance of security?

5.2 Internal Frequency Risk Factors

Internal Frequency Risk Factors are risk factors that are within your scope of control and that may affect the frequency of the risks you manage. These are factors that can be subject to an internal control.

- Will an attacker be successful a expoiting a vulnerability?
- How many software or architecture flaws do we have in our code or systems?
- How many unpatched and unmitigated vulnerabilities are there in third-party software we rely upon?
- How quickly can we patch software flaws in our systems?
- How many unsupported systems do we operate?
- How many suppliers do we trust?
- How exposed are our systems to exploitation?

- How quickly do our movers and leavers processes for our Identity & Access Management operate?
- How aware of security are our staff?
- How easy is it to impersonate our staff or our company?
- How often do we assure the effectiveness of our security controls and processes?
- Can we detect changes in staff stressors (financial, emotional, medical etc) and intervene effectively?
- Do our security staff have appropriate training and skills?
- Do we have enough security staff to meet our needs?

6 Risk Events

Risk events are events that can occur and may cause consequences.

We use Level 1 risk events to provide a convenient grouping of Level 2 events. We reccomend using the framework at the appropriate level of granularity with regards to the risk scenarios being considered.

Indicative impacts on the information security goals of Confidentiality, Integrity and Availability have been added where appropriate.

6.1 External Risk Events

External Risk Events are events that may occur outside your scope of control but may still cause consequences for your organisation or it's stakeholders.

Level 1	Level2	CIA
Supplier	Service Unavailability	Availability
	Service Compromise	Confidentiality, Integrity
	Information Breach	Confidentiality
	Access to Our System Breach	Confidentiality, Integrity
	Compliance Failure	
Regulatory	Rules Change	
Research	Critical Vulnerability Published	

6.2 Internal Risk Events

Internal Risk Events are events that may occur within your scope of control and cause consequences for your organisation or it's stakeholders.

The Internal Risk Events are largely derived from this ENISA [PDF] review of CSIRT incident taxonomies across Europe.

Level 1	Level 2	CIA
Abusive Content	Harmful Speech	
	Child / Sexual / Violent Content	
	Harassment	
Malware	Ransomware	Availability
	Worm	Confidentiality, Integrity, Availability
	Spyware	Confidentiality
	Rootkit	Confidentiality, Integrity, Availability

Level 1	Level 2	CIA
	Dialler	
Availability Interuption	Distributed / Denial of Service	Availability
	Sabotage	Integrity, Availability
Information Gathering	Open Source Intelligence Analysis	Confidentiality
	Network Scanning	
	Network Sniffing	Confidentiality
Social Engineering	Lies	Confidentiality, Integrity
	Threats	Confidentiality, Integrity
	Phishing	Confidentiality, Integrity
	Bribes	Confidentiality, Integrity
Information Breach	Unathorised access to system / component	Confidentiality, Integrity
	Unauthorised access to information	Confidentiality
	Unauthorised sharing of information	Confidentiality
	Unauthorised modification of information	Integrity
	Unauthorised deletion of information	Integrity, Availability
Fraud	Misappropriation / misuse of resources	
	False representation	
	Theft of money	
System Intrusion	Software Exploit	Confidentiality, Integrity
	SQL injection	Confidentiality, Integrity
	Cross-site scripting (XSS)	Confidentiality, Integrity
	File Inclusion	Confidentiality, Integrity
	Control System Bypass	Confidentiality, Integrity
	Use of stolen credentials	Confidentiality, Integrity

Level 1	Level 2	CIA
	Password brute force	Confidentiality, Integrity
Governance Failure	Process failure	Confidentiality, Integrity
	Audit Failure	Confidentiality, Integrity

7 Severity Risk Factors

Severity risk factors are relevant to the estimation of therange and severity of consequences that a risk event may cause to occur to occur.

7.1 External Severity Risk Factors

External Severity Risk Factors are risk factors that are outside of your scope of control that may affect the consequences of the risks you manage.

These are stated as questions to ask yourself or your organisation. The ability to estimate or measure these risk factors will vary between organisations.

- How much is the business worth?
- How many customers does the business have?
- What could be the level of fines we must pay?
- How much money will an attacker steal?
- What will be the cost for adverse legal action for negligence or liability?
- What would be the cost of reduced growth?
- What would be the cost of increased regulatory scrutiny?
- How much would customer notification cost?
- How much would customer rectification cost?
- Does our supplier have a documented & practised security incident response procedure?
- Does our supplier have a robust BC/DR capability?
- Does our supplier encrypt our data?

7.2 Internal Severity Risk Factors

Internal Severity Risk Factors are risk factors that are within your scope of control and that may affect the consequences of the risks you manage. These are factors that can be subject to an internal control.

- How long does it take us to detect financial crime?
- How long does it take us to detect security incidents from the initial attack stage?
- How long does it take us to resolve security incidents once detected?
- How much does it cost us to resolve security incidents?
- How often do we practice resolving breach scenarios?
- How many data records do we store?
- How long do we store data records for?
- How much money do we hold in our accounts?
- How much money can we access in our customers accounts?
- How many privileged user accounts do we operate?
- How much cyber insurance ocver do we have?
- How long does our BC/DR process take to resume and restore normal operations following a crisis?
- Do we encrypt our data?

- How long does it take us to onboard or switch suppliers?

8 Consequences

Consequences are the possible harm resulting from a risk event occuring including loss, injury, or other adverse or unwelcome circumstance.

The use of Level 1 consequences is just a convenient grouping.

Level 1 Consequences	Level 2 Consequences
Operations	Reduced growth
	Ineffective Change
	Slow recovery
	Reduced access to staff / skills
	Loss of suppliers
	Environmental harm
	Safety failure
	Social harm
	Medical harm
Compliance	Non-compliance
	Poor conduct / integrity
	Damaged regulator relations
	Regulatory fines
Financial	Theft of money
	Unplanned costs
	increased costs / inefficiency
Strategic	Damaged reputation
	Embaressing reporting
	Damaged investor relations