# A Cost-benefit Analysis of Information Security Mitigation Methods for ORVIs

Jake Street, Funminiyi Olajide
*Department of Computer Science, Nottingham Trent University, UK*

## Abstract

*In this paper we reviewed the cost-benefit analysis of Information Security and applied to Organisations Responsible for Vulnerable Individuals (ORVIs). Our research investigates the mitigation value and cost effectiveness of mitigation methods which discussed findings based on business focus and evaluation. Research findings indicated metrics for calculations assumptions, as proposed in the research work and thus, determined that the relative data analysis presented for cost comparable scores of the mitigation methods adopted. It is recommended from our analysis that ORVIs implement Internal Penetration Testing alongside Policy implementation due to the added benefit this combination has for this specific use-case.*

*Keywords: ORVIs, Information Security, Vulnerable Individuals, Mitigation Methods, Cost-benefit Analysis*

## 1. Introduction

The attacks that are encounter by organisations are directed to the Confidentiality, Integrity, and/or Availability of information. Organisations tend to be targeted over Personal/Independent users by cybercriminals due to the ability to make a greater financial gain than from targeting Personal users. Financial gain was found to be the most common motive amongst attackers with, depending on the attack method used, 64-100% of attacks having a financial motive [2]. As these attackers tend to make financial gains on a successful attack, the organisation that is the victim of the attack will be negatively impacted financially, sometimes a greater loss than what was gained by the attacker. As well as this, organisations have a legal responsibility to keep sensitive information secure as well as reporting a breach. However, this breach reporting has been known to have a significant negative effect on the share price of the organisation [3]. Because of these reasons it is advised that most organisations implement mitigations to reduce the likelihood of these attacks occurring or reduce the damage of the attack if it were to occur. However, for business-focused management within organisations, the implementation of these mitigation methods can be significantly expensive. Therefore, an organisation attack that may seem too unlikely to be worth mitigating, it is the role of the IS team within an organisation to demonstrate the value of investing within IS and the risk of not investing.

Despite the asset-based approach that most IS quantitative and qualitative analysis follows there are further needs of some organisations (and certain individuals) that should be addressed when creating their IA plan. All of these additional needs have a monetary impact on an organisation, with some being direct and some indirect. The first of these additional needs is Legal considerations. These legal considerations need to be followed by the organisation to mitigate the risk of prosecution, which can involve a monetary fine for the organisation or in serious circumstances be treated as a criminal matter and lead to prison sentences for the accountable individuals/entities. These legal considerations can be either of a general nature, which refers to laws that almost all organisations need to comply with regardless of sector e.g., EU organisations processing personal data to comply with the General Data Protection Regulation [16], or of a more specific nature, which are often sector specific laws that only organisations that conduct a specific business process must comply with.

The next additional need are social considerations made by organisations to protect the intangible asset of ‘trustworthiness’ and the public’s perception of the organisation which are likely to be damaged in the event of an attack. This need is often addressed within the asset-based analysis; however, it can be very difficult to quantify the possible damage that an attack on this would cause as well as the value that this asset is giving to the organisation. The final need that should be addressed are ethical considerations. While ethical issues are unlikely to cause a direct and immediate impact on the organisation’s financials, regular and severe infringements of an ethical nature are likely to cause moral repercussions on employees. Based upon the extent of the issue within the organisation this could lead to employee whistleblowing, which is likely to cause financial loss to the organisation due to damage to the intangible assets of trustworthiness and the public’s perception of the organisation. It is suggested that for both social and ethical considerations the amount of damage caused to a given organisation is likely to vary significantly from sector to sector. This is due to the differences in the value of the intangible asset of ‘trustworthiness’ and public’s perception of the organisation, as the value of this intangible asset is greater for larger organisations (who traditionally have a larger customer base) it is suggested that business size is directly proportional to the damage caused by a social/ethical issue (with the industry sector acting as a ‘baseline’). An example of an industry with a very high reliance on organisation trustworthiness is within cyber security. For example, following the breach suffered by the Certificate Authority company ‘DigiNotar’ was forced to declare bankruptcy due to a lack of trustworthiness from the public and trustworthiness of major internet browsers [17].

In this paper, we highlighted the common attacks facing organisations, common pre-attack mitigation methods, and then provide a cost-benefit analysis to identify the methods that provide the most mitigation effectiveness for the lowest cost. Within the ‘Overview of Attacks’ section six common IS attacks that face organisations will be discussed and a severity rating of ‘Low’ or ‘High’ will be assumed. The findings from this section will be cross analysed with the effectiveness of seven common pre-attack mitigation methods implemented by organisations, to give a ‘Mitigation Value’ (MV) score. This score will then be compared to the average assumed price of implementation, determined in the ‘Overview of Common Mitigation Methods’ section to work out a ‘Cost Comparable Score’, with the lower the score meaning the more cost effective the mitigation method is for both general organisations and for ORVIs to compare the differences in their cost-effective approach.

## 2. Literature Review

In this section will cover the ‘Attacker’s Motives for Attacking ORVIs’, which will provide understanding as to the exact value gained by the attacker conducting the attack which in turn will provide awareness as to the attack method selected by the attacker. The ‘Overview of General IS Attacks’ sub-section shall detail the common Information Security attacks experienced by organisations regardless of sector, whereas the ‘Overview of Specific IS Attacks Facing ORVIs’ shall provide the same analysis but with a focus on ORVIs. The literature review will conclude with the ‘Overview of Common Mitigation Methods in a General and ORVI-Centric Context’ which will give an overview as to the mitigation methods often employed to mitigate these attacks as well as any considerations commonly made by ORVIs or general organisations while implementing a given method.

### 2.1. Attacker’s Motives for Attacking ORVIs

Most attacks against organisations have a common motive and amongst attackers are the ability to make financial gains. Whereas the financial gain from conducting an attack against an ORVI is likely to be the same compared to other organisations, the financial damage is likely to be a lot greater for ORVIs. This is due to the additional considerations (Legal, Social, and Ethical considerations) that ORVIs need to consider when creating there is plan. However, because of these factors ORVIs may find themselves more suspectable to attackers who are aiming to cause the most amount damage to an organisation and are not aiming for direct financial gain from the attack. These attackers can have this motivation for a variety of reasons, for example a disgruntled employee, a competitor of the organisation knowing that the damage would aid their organisation, or a recreational attacker who is looking to cause as much damage for fun.

An additional attack vector for ORVIs needs to be considered; the vulnerable individuals themselves. The exact degree of responsibility to protect their vulnerable individuals a given ORVI faces is often on a case-by-case basis, and often is based upon the circumstances of the attack. For example, if we were to consider a school, most people would agree that an attack facing a child while they were at school would be the responsibility of the school. Conversely if the attack were to happen at the child’s home, most people would agree that it is not the responsibility of the school. However, within this there are many grey areas that need to be considered, following this example if the child were to experience an attack while travelling to or from school there is a degree of uncertainty as to where the burden of responsibility lies. Within the additional attack vector, some further attacks are likely. As previously mentioned, it was suggested that the likelihood of an attacker attacking an ORVI for their own financial gain is about the same as for any other organisation, however the same is not true for attacks against the vulnerable individuals for financial gain. As these vulnerable individuals are likely to have one or more of the following attributes: lower risk/attack awareness, lower technical ability, and are unable to understand the meaning/context of certain events.

An additional consideration that needs to be made for ORVIs is attacks surrounding the attacker’s motive of sexual gratification. The vulnerable individuals within ORVIs are often targeted for these attacks as they are often unlikely to understand the implication of following the instructions of the attacker or why it is ‘wrong’, and therefore from an attacker’s perspective the likelihood of their attack succeeding is increased by targeting these individuals. These attacks can either form in a coercive manor or a more aggressive manor. Most of the coercive methods used by the attacker involve deceiving the vulnerable individual into thinking they have formed a romantic relationship with the attacker or have formed a close friendship. However, despite this being ethically wrong if done to non-vulnerable individuals legal, social, and more ethical issues arise for the ORVI when this is targeted at a vulnerable individual instead. This is often the case as the vulnerable individuals are often legally unable to give consent for sexual acts. This could be due to any of the following factors: the given individual is under the age of eighteen, in which it is illegal for the individual to transmit sexual media; the given individual is under the age of 16, in which they cannot give consent for sexual acts; or the individual is unable to make their own decisions under the Mental Capacity Act 2005 [18], which can often be determined in the context of sexual relationships by the individual completing an 'Assessment of Sexual Knowledge' (ASK) [19].

## 2.2. Overview of General IS Attacks

The first IS attack is an 'Insider' attacks. This attack can target any, but not necessarily all, of the information security principles (Confidentiality, Integrity, and Availability). This attack is defined as any attack carried out by an internal, or trusted, entity within an organisation, most commonly a disgruntled employee either sharing intellectual property (IP) to a business competitor or an emotionally driven attack against another employee. The severity of this attack is dependent on the target of the attack (IP is likely to be very severe whereas a dispute amongst employees is unlikely to cause a significant impact on business operations), and the detectability/accountability of the attack (a detectable IP attack, and usage of digital forensics, can result in legal action to recoup any losses from the attackers). Therefore, from an IS approach, Insider attacks will be deemed to have a high severity.

The 'Social Engineering' attacks are IS based that requires an attacker to use social cues or deception to gain information. As these attacks involve conversing with people within an organisation, social engineering has a high risk for the attacker and therefore, Social engineering attacks are often used in combination with another attack method, e.g., Physical security attacks, to avoid outright detection.

Physical Security Attacks relate to the exploitation of physical vulnerabilities within an organization's assets. A common physical attack could involve picking a door lock to gain physical access to significant organisational infrastructure e.g., a server room. Common Physical IS attacks tend to involve an attempt to gain physical access to infrastructure to then implement a piece of malicious hardware, as a 'set-up' to another attack, or even aim to overhear/observe the significant information targeted. As these attacks are often used as a reconnaissance attack, are often easily attack-evident, and are often not fully directly mitigatable against a committed prepared attacker this attack shall be considered low severity.

Vulnerability Exploitation Attacks rely on exploiting vulnerabilities in software and hardware that haven't been patched, these vulnerabilities can range from widely known vulnerabilities (e.g., SQL injection attacks) to more bespoke attacks or zero-day vulnerabilities. The attacker can have a wide range of motives for an attack of this type, based on the asset attacked. This attack can affect any of the information security principles and is often not attack-evident, therefore this attack is assumed to be of high severity.

Malware is the general term given to any malicious software on a system, this can range information harvesting tools such as keyloggers to information destructive tools such as ransomware. Alike Vulnerability Exploitation Attacks, the motives of an attacker are varied due to the vast volume of possible attacks under the category of malware, which also makes the assumed severity of this attack high.

## 2.3. Overview of Specific IS Attacks Facing ORVIs

The specific considerations of ORVIs are based on additional risks and attacks that they and their vulnerable individuals face. Despite these attacks being bespoke in nature the attacks, as well as the mitigation methods, can still be categorised under the same IS approaches as followed by most organisations. Therefore, each of the general IS can be used to categorise the specific attacks facing ORVIs.

'Insider' attacks are one of the most common attacks that ORVIs face. This is defined as an internal attacker, often an employee of the ORVI, attacking a vulnerable individual. This is due to the trust and power given to these employees in fulfilling their role which in turn opens the door for possible exploitation. These attacks can range from sexual exploitation, such as coercive grooming, aggressive sexual assault, or techniques like blackmail; financial exploitation, from having access to the vulnerable individual's bank accounts/assets; or even with voter fraud, in which an attacker can use the proxy vote system to vote on behalf of an individual, possibly without their knowledge, in an attack sometimes referred to as 'granny farming' [20]. Because of the variety of attacks and the likelihood and impact of the attack occurring, this attack has the greatest risk to ORVIs.

The 'Social Engineering' attacks are similar in nature to 'Insider' attacks in this context. These attacks are conducted by an external individual, who has scouted the vulnerable individual from some form of reconnaissance. The exploitation is the same as for 'Insider' attacks, however these attacks are likely to be less prominent/successful as this attack requires reconnaissance and the attacker is not already in a position of power, unlike with ‘Insider’ attacks. However, ‘Social engineering’ attacks do differ from ‘Insider’ attacks in terms of the attack vector used, where ‘Insider’ attacks will tend to conduct their attacks in-person, ‘Social engineering’ attacks are likely to be mixed between the in-person and Internet-connected device attack vector.

The ‘Physical’ attacks against ORVIs are very similar in nature to physical attacks against most organisations however how they differ is in the asset that they are protecting. Whereas most general organisations will be defending a critical piece of technical infrastructure, a technical or non-technical system that holds sensitive documents, or assets of resale value that can be stolen. Physical attacks against ORVIs are often targeted at the vulnerable individuals themselves by the attacker circumventing physical defences (e.g., doors) to gain access to the vulnerable individual. It is also possible that the physical attacks could be of a reconnaissance nature, but this is only common in organisations that rely heavily on paper-based documentation and/or have little technical systems. There are specific challenges when it comes to physical attacks against individuals in both the attack sense, and the mitigation sense. For the attacker it allows them to become uniquely identifiable and it is likely that sufficient evidence will be easily gathered against them (using commonplace systems such as CCTV), which is often not the case with attacks done away from site. Additionally, unless reconnaissance is done there is no way to have certainty of where the vulnerable individual is. Because of these factors there is significant risk of detection for the attacker, however this does not necessarily mitigate the attacks. It is suggested, however, that this changes the characteristics of the attacks with them tending to be ‘stand-alone’ and less complex in their design.

Attacks that are based on installing malicious code or exploiting vulnerabilities on the vulnerable individuals, or ORVI’s, devices are likely to be used against ORVIs to create the most amount of damage against the organisation. If the vulnerable individual is the target of this attack, then it is likely that these would be used for reconnaissance purposes or to be able to blackmail the vulnerable individual from having access to their personal files. However, because of the latter, these types of attacks are less severe to ORVIs than some of the others mentioned.

## 2.4. Overview of Common Mitigation Methods in a General and ORVI-Centric Context

Infrastructure design is another mitigation method, which is an umbrella term for a variety of network design choices and implementable hardware/software. Examples of this involve; Firewalls, which drop or accept packets which match certain conditions; Intrusion Detection Systems, which aim to detect if a hacker has infiltrated a computer system through the network; Designing computer networks with security in mind, to reflect security methodologies such as Access Control Layers [5] based on how critical the information is.

In terms of infrastructure design, a firewall can be practically free if only needed for low-load networking as a low-end or depreciated computer system can be used with an open-source piece of firewall software with the only costs being electricity costs, staffing costs, and purchase of a computer system if a depreciated system is not available. However, for a more high-load networking solution, an organisation can purchase a dedicated firewall solution. For a medium range firewall this can range from £1,144-£3,814 [6], for both the hardware and software. In terms of the use of infrastructure within ORVIs, as this is purely a technical mitigation method it is not as well suited to the types of attacks that ORVIs are likely to face.

The Anti-malware mitigation method involves using a piece of software to analyse of files on a computer system to identify if there are any ‘signature matches’ to known pieces of malware, or a more Heuristic approach by analysing the computers behaviour against a baseline to indicate if the computer is behaving suspiciously.

Many anti-malware software solutions can be implemented for free but often these types of software may not possess the features/technical support that organisations may require. Additionally, it is likely that it’s contractually stipulated that the software is to only be used for non-commercial use. It is suggested that most anti-malware solutions cost around £23-£61 per license per year [7] however some Anti-malware companies may reduce this cost based on the quantity of software licenses ordered.

Similarly, to the ‘Infrastructure’ IS mitigation method, when it comes to mitigating the attacks that ORVIs tend to experience Anti-malware software is likely to not have a significant effect due to the technicality of the solution.

Training employee on mitigation method involves educating members of staff against common attacks and gain an awareness of security as a concept. This can be done by having staff complete a certification/exam, having an external training provider give a seminar, or merely encouraging open discussion about the topic of information security. These qualifications can range from free, online qualifications, to funding a degree/apprentice. For an employee to cover Information Security Awareness training it costs around £495 (Learning Tree, 2019).

Employee training for ORVIs is likely to be effective, presuming that it is bespoke to the ORVI. This is because it will directly address the attack

Copyright © 2021, Infonomics Society | DOI: 10.20533/jitst.2046.3723.2021.0092

most likely to occur (‘Insider’) as well as other high probability attacks (‘Social Engineering’). This mitigation method also has the added benefit of acting as a deterrent to possible attackers, this is due to prospective attackers having to attend the training and knowing that their colleagues will be vigilant to attack attempts, thus reducing the probability of an attack and the overall risk, as well as the clear detective measures imposed by giving this training.

Policy publication can be implemented as a technical or non-technical solution, with technical solutions including the use of website filtering and file/directory access controls. These non-technical policies can include Bring-your-own-device policies, General Acceptable Usage policies, and a Code of conduct [1]. These mitigation methods are completely free, not accounting for the employee time to create these documents. Some organisations may decide to outsource this operation, however there are many free templates online and it is recommended that this method is best done in-house to ensure a bespoke policy is created which is likely to be followed by employees.

Theoretically policy publication is likely to be effective at mitigating the attacks commonly faced by ORVIs, however in the real-world implementation this may not be the case. This is due to the possibility that employees may just choose not to follow the policy in some circumstances, there may be a poor security culture at the organisation, or the policy is not communicated effectively with the staff by the responsible individual.

Penetration testing (Pen Test) as a mitigation method involves an external ethical attacker to attempt to break into your system and produce a report which identifies the vulnerabilities within the organisation’s IS strategy, as well as recommendations on whether to Reduce, Accept, Transfer, or Eliminate the risks identified [1].

Many factors impact the price of a penetration test, such as the complexity of the system being tested and the cost of any additional penetration tools that may be needed to conduct the penetration test [8]. Despite the cost of this mitigation method varying significantly, it is predicted that the outright cost of a penetration test is £5,409 [9], with likely post pen test costs of £5,769. Therefore, the average cost of this method is £11,178.

In the context of attacks specific to ORVIs, Pen Tests can be used in a variety of ways to mitigate the risk posed by these attacks. These Pen Tests can be used in the ‘traditional’ way with the penetration tester conducting an attack as a social engineer and identifying if the other implemented mitigation methods are effective e.g.,, Physical, Employee Training. However, a different approach to this would be having the penetration tester join the organisation as an employee and attempt ‘Insider’ attacks, not only would this give a better judgement of how effective the Staff Training mitigation method is, but it also provides the penetration tester with the ability to observe policy compliance from employees as well as the overall security culture of the organisation. It is suggested by using this version of a penetration test would prove most useful to ORVIs as it allows a real-world view of the policy implementation as well as identifying possible attack methods that ‘Insiders’ could use.

Information Risk Management standards (IRM) involves an organisation complying with given Information Security standards. A common IS standard the International Organization for Standardization’s (ISO) ‘27000’ family standards [10], which detail the controls that organisations should meet to ensure information is kept secure, or the British Standard Institution (BSI) 7799-3:2017, which aims to aid information security auditors and to ensure that organisations are complying with the GDPR legal requirements [11].

In order to be certified, an organisation must pay a fee for the first audit and are required to pay for further audits in the future. This is to ensure the IS standards are continually being upheld, as well as changes are being made upon discovery of new threats. The price of an Information Risk Management Standards Audit is proportional to the number of employees working in the organisation. The cost a complete audit, of ISO 27001, can range from £2,850-£14,250 [12]. As standards are well-defined, there is little to no scope for changing these controls to the context of ORVIs and therefore despite addressing most of the general attacks, this mitigation method is ineffective at specific use-cases such as this one.

## 3. Calculations

As with any cost-analysis comparison it is unlikely that there will be a ‘like-for-like’ direct comparison, due to external variables. The sub-section ‘Calculation Assumptions’ shall analyse these additional variables and make adjustments to the calculations, so that a fairer comparison can be made between each mitigation method. The ‘Analysis’ sub-section shall determine the cost-comparable score for each mitigation method for both general organisations and ORVIs based upon the assumed mitigation effectiveness and assumed severity score.

### 3.1. Calculation Assumptions

The literature that provided mitigation quote estimations in other currencies these have been converted as follows based upon currency conversions on the 9th of September 2021, as shown below.

- $1 (USD) : £0.72 (GBP)

We assumed in the calculations that all mitigation methods requiring hardware will follow a four-year depreciation cycle [4].

For anti-malware and staff training, it was assumed the organisation is a medium sized organisation which is categorised as having 50-249 employees [13]. Taking the mean of this range gives us 150 employees, with each employee having one dedicated workstation i.e., 150 licenses.

It is common for staff training courses to require renewal after four years [14], we assumed that staff training is effective for a period of four years.

Penetration testing is required yearly as per requirement 11 of PCI DSS [15], however it should be noted that complying to the standard is not required to have Penetration Tests.

The 'IRM Standards' mitigation methods, have not considered additional costs within the above calculations that may be incurred following an assessment.

### 3.2. Analysis

The Table 1 shows the assumed Mitigation Effectiveness (ME) of each of the described mitigation methods within the 'Overview of Common Mitigation Methods' section against each IS attack detailed within the 'Overview of Information Security Attacks' section for both general attacks and attacks specific to ORVIs. Each method is given one of three ratings for each attack, as follows:

Table 1. Assumed Mitigation Effectiveness

| Attacks | Mitigation Methods | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | *Infrastructure* | | *Anti-malware* | | *Training* | | *Policy/Access* | | *Pen Test* | | *IRM Standards* | |
| | *General ME* | *ORVI ME* | *General ME* | *ORVI ME* | *General ME* | *ORVI ME* | *General ME* | *ORVI ME* | *General ME* | *ORVI ME* | *General ME* | *ORVI ME* |
| 'Insider' | N | N | N | N | P | Y | Y | Y | N | Y | Y | N |
| Social Engineering | N | N | N | N | Y | Y | Y | Y | Y | Y | Y | N |
| Physical | P | N | N | N | N | N | N | N | Y | Y | Y | Y |
| Vulnerability | Y | Y | N | N | N | N | P | N | Y | Y | Y | Y |
| Malware | P | P | Y | Y | P | N | P | N | P | P | P | P |

- 'No' (N) – Used to denote mitigation methods that have little to no mitigating effect on the attack.
- 'Partial' (P) – Used to denote mitigation methods that are designed to mitigate certain elements, but not all, of a given attack or a mitigation method that was not designed to mitigate a given attack but has a partial mitigating effect.
- 'Yes' (Y) – A mitigation method that was designed to mitigate the given attack, however this may not be the sole function of the mitigation method.

Table 2. Cost Comparable Score Calaculation – General organisations

| Attacks | | Mitigation Methods | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | *Infrastructure* | | *Anti-malware* | | *Training* | | *Policy/Access* | | *Pen Test* | | *IRM Standards* | |
| | *General Severity* | *ME* | *MV* | *ME* | *MV* | *ME* | *MV* | *ME* | *MV* | *ME* | *MV* | *ME* | *MV* |
| 'Insider' | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 4 | 0 | 0 | 2 | 4 |
| Social Engineering | 2 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 4 | 2 | 4 | 2 | 4 |
| Physical | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 0 |
| Vulnerability | 2 | 2 | 4 | 0 | 0 | 0 | 0 | 1 | 2 | 2 | 4 | 2 | 4 |
| Malware | 2 | 1 | 2 | 2 | 4 | 1 | 2 | 1 | 2 | 1 | 2 | 2 | 4 |
| *Total Mitigation Value (Total MV)* | | 9 | | 4 | | 6 | | 12 | | 13 | | 17 | |
| *Mean Cost / Year* | | £620 | | £6,300 | | £18,563 | | £0 | | £11,178 | | £2,850 | |
| *Cost Comparable Score* | | £68.89 | | £1,575.00 | | £3,093.83 | | £0 | | £859.85 | | £167.65 | |

Table 2 shows the Mitigation Value (MV) by multiplying the values of the Severity of the attack within the 'Overview of Information Security Attacks' section, with low severity being given one point and high severity being given two points, and the ME from Table 1; with 'No' being given zero points, ‘Partial’ being given one point, and ‘Yes’ being given two points. Following on from this the mean cost of mitigation implementation, determined from the Literature analysis within the ‘Overview of Common Mitigation Methods’ section, is then divided by the Total Mitigation Value (Total MV) to calculate a Cost Comparable Score which aims to demonstrate the mitigation value for money (the pound cost to get one MV point). Table 3 follows the same methodology as the calculations in Table 2, but only evaluates the effectiveness in terms of ORVI-specific attacks.

Table 3. Cost Comparable Score Calaculation – ORVI-specific

| **Attacks** | | **Mitigation Methods** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ***Infrastructure*** | | ***Anti-malware*** | | ***Training*** | | ***Policy/Access*** | | ***Pen Test*** | | ***IRM Standards*** | |
| | ***Severity to ORVIs*** | ***ME*** | ***MV*** | ***ME*** | ***MV*** | ***ME*** | ***MV*** | ***ME*** | ***MV*** | ***ME*** | ***MV*** | ***ME*** | ***MV*** |
| Insider | 3 | 0 | 0 | 0 | 0 | 2 | 6 | 2 | 6 | 2 | 6 | 0 | 0 |
| Social Engineering | 2 | 0 | 0 | 0 | 0 | 2 | 4 | 2 | 4 | 2 | 4 | 0 | 0 |
| Physical | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 4 |
| Vulnerability | 1 | 2 | 2 | 0 | 0 | 0 | 0 | 0 | 0 | 2 | 2 | 2 | 2 |
| Malware | 1 | 1 | 1 | 2 | 2 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| ***Total Mitigation Value (Total MV)*** | | 3 | | 2 | | 10 | | 10 | | 15 | | 6 | |
| ***Mean Cost / Year*** | | £620 | | £6,300 | | £18,563 | | £0 | | £11,178 | | £2,850 | |
| ***Cost Comparable Score*** | | £207 | | £3,150 | | £1,856 | | £0 | | £745 | | £475 | |

## 4. Discussion

The  Tables 2 and 3 show that the key differences between general organisations and ORVIs in terms of the Information Security mitigation methods should be considered for implementation, for both organisations that have budget considerations and organisations without.

As shown by the ‘Severity’ attribute in both Tables 2 and 3, a different approach is required to be taken by both general organisations and ORVIs when constructing an IA plan. The severities, which have been assumed from the likelihood and impact of the attack, for general organisations are mostly consistent throughout the scope of attacks within this paper. This can be attributed to the ‘Reconnaissance’ phase, which is common in most planned attacks against general organisations, that involves the attackers analysing the organisation’s defensive measures to identify any vulnerabilities. Therefore, a general organisation requires coverage against all attacks. It should be noted that the ‘Physical’ attack has been given a lower severity due to the additional risk for attackers conducting Reconnaissance for this given attack method, as there is a material threat of detection for the attacker by carrying out reconnaissance for a physical attack due to the in-person, and thus non-repudiation nature of this activity.

Conversely, as the attacks targeted at ORVIs tend to be bespoke in nature, often there have been only few possible attack methods providing the attacker with their target. The IA plan can be tailored to do the latter and does not necessarily require complete coverage (despite being recommended in most use cases). The common factor between  the attacks targeted at ORVIs is that they  are  all  conducted in-person. This is a ‘double edged sword’ for  ORVIs, as there is a greater chance of identifying the attacker, but it is likely that intruders conducting attacks are aware of this and have analysed and accepted this risk. Because of this a IS strategy that relies on deterrents against these attackers is likely to be less effective than against attackers who are targeting general organisations.

## 5. Recommendations

Recommendations for General Organisations - From the analysis carried out in Table 2, the most cost-effective method is ‘Policy Publication and Access Control’, as there are no direct expenses to implement this mitigation method with this method giving significant MV.

The next best mitigation methods in terms of value for money are ‘Backups’ and ‘Infrastructure’. These mitigation methods are recommended as cost-effective methods to combat attacks focused on disrupting the availability of critical data. However, this may not be a complete solution against availability attacks that are Internet-facing services accessed by customers.

On the other end of the scale, the ‘Staff Training’ mitigation method is significantly more expensive than the other methods analysed and provides poor value for money due to this method only truly mitigating Social Engineering attacks (however, the true effectiveness of this method for these attacks is disputed). This mitigation method is discouraged in organisations of all sizes with budget considerations, other than in organisations in which social engineering attacks are of high probability e.g., a bank.

For organizations with greater budgets, it is recommended that the ‘IRM Standards’ and ‘Penetration Testing’ mitigation methods are implemented. This recommendation is based on the findings presented in Table 2, these methods are the gold standard in ensuring good coverage against the full variety of IS attacks. From the analysis of Table 2 the ‘Anti-malware’ mitigation method does not appear to provide enough value for the implementation cost to be considered especially due to other mitigation methods giving partial mitigation against these attacks. It is recommended that organisations conscious of their budget, consider alternative methods to mitigate the threat of malware either by installing a dedicated piece of open-source Anti-malware software, using a combination of the methods discussed in this paper, by using an operating system with in-built Anti-malware software, or by using operating systems that are not as susceptible to malware e.g., Linux.

An observation that can be made from these recommendations is the ‘bell-like curve’ in terms of the outsourcing of these IS mitigation methods. For example, based on the findings from Table 2, it appears to be preferable for organisations with a low budget to implement in-house solutions, such as Policy/Access Control and Infrastructure. Conversely, based on Table 2, organisations with a medium sized budget are likely to use methods which require outsourcing for example, Penetration Testing and IRM Standards. It is theorized that, organisations with a larger budget will tend to bring these outsourced activities back in house, for example by hiring a dedicated in-house IA team or by hiring a dedicated penetration tester.

Recommendations for ORVIs - As shown by the disparity amongst the Cost Comparable Scores for some of the mitigation methods as shown in Figure 1 and by Table 3, a different approach is required for ORVIs in terms of cost-effectiveness of IS mitigation methods. Somewhat similarly to the general recommendation, it was found that Anti-Malware software is cost ineffective for ORVIs as well as IRM standards being more cost ineffective than for general organisations. This was primarily due to these mitigation methods not addressing the risks that were most pertinent to ORVIs. Conversely to this, however, Staff Training as well as Penetration Testing were both more cost effective for ORVIs than general organisations due to the nature of these mitigation methods being more (or having the opportunity to be more) targeted towards the risks faced by ORVIs.

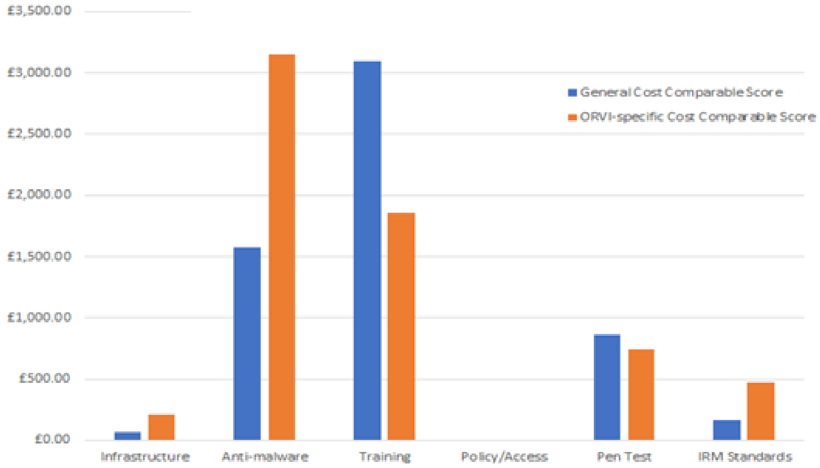

Figure 1. Cost Comparable Scores General vs. ORVIs

Our analysis shows that the ORVIs must implement Policy Controls and conduct regular Internal Penetration Tests (to test how secured is the system against Insider attacks and Social Engineering attacks), but also to identify if Policy is being followed and suggesting actions if this is not the case and/or to identify possible issues within the organisation’s security culture.

## 6. Conclusion

The literature review and cost-benefit analysis in Table 3 attacks targeting ORVIs tends not to be of a technical nature and are mostly conducted in-person, with a large proportion of attackers working for the ORVI. Therefore, as well as the cost considerations, emphasis for ORVI’s IA plan should involve well-designed processes which encourages whistleblowing, independent auditing, and a culture in which no individual or group within a ORVIs is trusted.

For all organisations ‘IS Training’ is often not justified in terms of the cost-benefit it provides and should only be considered for implementation for organisations that experience IS attacks very commonly. This should not, however, be confused with implementing policies within an organisation which is recommended, based upon the cost-benefit analysis, for all organisations despite requiring some level of in-house training/revision of the policy.

## 7. References

[1] Taylor, A., Alexander, D., Finch A. and Sutton, D. (2020). Information security management principles. 3rd ed., British Computer Society, January 2020.

[2] Verizon Communications. (2021). Data Breach Investigations Report. https://enterpriseVeri zon.com/ resources/reports/2021-data-breach-investigations-report.pdf (Access Date: 7 September 2021).

[3] Rosati, P., Deeney, P., Cummins, M., van der Werff, L. and Lynn, T. (2019). Social media and stock price reaction to data breach announcements: Evidence from US listed companies", Research in International Business and Finance, vol. 47, pp. 458-469, DOI: 10.1016/j.ribaf.2018 .09.007.

[4] Nolle, T. (2021). Evaluating the useful life of a server. Excess Logic. http://excesslogic.com/electroni cs/evaluating-the-useful-life-of-a-server/. (Access Date: 11 September 2021).

[5] Sandhu, R. and Samarati, P., (1997). Authentication, Access Controls, and Intrusion Detection. The Computer Science and Engineering Handbook.

[6] Shinder, D. (2004). Choosing a Firewall. TechGenix. https://techgenix.com/choosing_a_firewall/. (Access Date: 12 September 2021).

[7] Electronics Costhelper. (2021). How Much Does Anti -Virus Software Cost?", CostHelper, https://electronics.costhelper.com/anti-virus-software. (Access Date: 12 September 2021).

[8] Hub Hacken. (2021). Penetration Testing Cost | Pen Testing Pricing, Hacken. https://hub.hacken.io/blog /how-much-does-penetration-test-cost-or-price-ofyoursecurity. (Access Date: 12 September 2021).

[9] Outpost24. (2021). The Economics of Penetration Testing for Web Application Security, https://outpost 24.com/sites/default/files/2019-06/Economics-of-Pen-Testing-Whitepaper.pdf. (Access Date: 12 September 2021).

[10] IT Governance. ISO 27000 Series of Standards. (2021). https://www.itgovernance.co.uk/iso27000-fa mily. (Access Date: 12 September 2021).

[11] Legislation Gov UK. (2018). Data Protection Act. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (Access Date: 12 September 2021).

[12] IT Governance. (2021). Typical ISO 27001 certifica tion costs. https://www.itgovernance.co.uk/iso27001-certification-costs. (Access Date: 12 September 2021).

[13] Department for Business, Energy, and Industrial Strategy. (2019). Longitudinal Small Business Survey: SME Employers (1-249 employees). UK.

[14] SANS. (2021). Introduction to Cyber Security Train ing Course | SANS SEC301. https://www.sans.org/cyber-security-courses/introduction-cyber-security/. (Access Date: 12 September 2021).

[15] Pcisecuritystandards. (2021). PCI DSS Standard. https ://www.pcisecuritystandards.org/document_library. (Access Date: 12 September 2021).

[16] General Data Protection Regulation (GDPR). (2018). Final text neatly arranged. https://gdpr-info.eu/. (Access Date: 27 November 2021).

[17] Van der Meulen, N. (2013). Diginotar: Dissecting the first dutch digital disaster. Journal of strategic security, vol 6, no 2, bll 46–58.

[18] Legislation Gov UK. (2005). Mental Capacity Act. https://www.legislation.gov.uk/ukpga/2005/9/contents. (Ac -cess Date: 29 November 2021).

[19] Galea, J., Butler, J., Iacono, T., Leighton, en D. (2004). The assessment of sexual knowledge in people with intellectual disability. Journal of Intellectual and Developmental Disability. vol 29, no 4, bll 350–365.

[20] News BBC. (2005). Row over Alzheimer woman's proxy. http://news.bbc.co.uk/1/hi/uk_politics/vote_20 05/england/4510971.stm. (Access Date: 29 November 2021).