A picture containing text, queen

Description automatically generated

Edge Hill University

The Department of Computer Science

CIS4124 – Information Security Management

Level 7

Report 1

REPORT TO SUPPORT LEADING EDGE REMOVALS EXPAND THE BUSINESS SECURELY.

Report 2

Incident Response

Contributors:

Callum McLaughlin, Lewis Patterson, Paul Jacka, Priyanka Saini, Roma Mudasar, Syed Azlan, William O’Shea-Metcalfe

THIS PAGE IS LEFT BLANK INTENTIONALLY

[1. Introduction 1](#_Toc121255910)

[2. A plan for influencing the board (actions/supporting information needed/presentation) 1](#_Toc121255911)

[2.1 Influencing the Board 1](#_Toc121255912)

[2.2 Actions and Supporting Information 2](#_Toc121255913)

[3. An assessment of the key features of ISO27001 and Cyber Essentials and their suitability for this company. 3](#_Toc121255914)

[3.1 Cyber Essentials 3](#_Toc121255915)

[3.2 The five controls are: 3](#_Toc121255916)

[3.2.1 Use a firewall to secure your internet connection: 3](#_Toc121255917)

[3.2.2 Choose the most secure settings for your devices and software: 3](#_Toc121255918)

[3.2.3 Control who has access to your data and services: 3](#_Toc121255919)

[3.2.4 Protect yourself from viruses and other malware: 4](#_Toc121255920)

[3.2.5 Keep your software and devices up to date: 4](#_Toc121255921)

[3.3 International Standards Organisation 27001 (ISO27001) 4](#_Toc121255922)

[3.4 Mandatory ISO 27001 requirements 5](#_Toc121255923)

[3.5 ISO 27001 mandatory clauses: 5](#_Toc121255924)

[3.6 ISO 27001 vs Cyber Essentials: 6](#_Toc121255925)

[3.6 Suitability of Cyber Essentials Plus and ISO27001. 7](#_Toc121255926)

[4. A detailed proposal for securing the company assets and developing a security culture. 8](#_Toc121255927)

[4.1 Overview of Current Security 8](#_Toc121255928)

[4.2 How Could Security be improved at the company? 8](#_Toc121255929)

[4.3 Risk Identification Table 9](#_Toc121255930)

[4.3.1 Figure 1: Risk table 11](#_Toc121255931)

[4.4 Asset Risk Matrix 12](#_Toc121255932)

[4.4.1 Figure 2: Risk Matrix 12](#_Toc121255933)

[4.5 ROSI 12](#_Toc121255934)

[5. Recommendations 13](#_Toc121255935)

[5.1 Prioritisation. 13](#_Toc121255936)

[5.1.1 Instil the concept that security belongs to everyone – Risk 6. 13](#_Toc121255937)

[5.1.2 Obtaining support from Senior Leadership – Risks 1–6. 13](#_Toc121255938)

[5.1.3 Information Technology Improvements 13](#_Toc121255939)

[5.1.4 Accounting System – Risk 1. 13](#_Toc121255940)

[5.1.5 Transfer email hosting to the cloud 14](#_Toc121255941)

[5.1.6 External Threat Prevention – Risk 1,3-6. 14](#_Toc121255942)

[5.1.7 Servers Improvements – Risk 4 14](#_Toc121255943)

[5.1.8 Moveware – Risk 3. 14](#_Toc121255944)

[5.1.9 Warehouse Localities – Risk 2. 14](#_Toc121255945)

[5.1.10 Staff - Risk 6. 14](#_Toc121255946)

[6. References: 15](#_Toc121255947)

[7. Introduction 18](#_Toc121255948)

[8. Initial Event 19](#_Toc121255949)

[8.1 Is this classified as an incident? 19](#_Toc121255950)

[8.2 Information required 19](#_Toc121255951)

[8.3 Likely damage to Edgecoin 20](#_Toc121255952)

[8.4 Future risk if not resolved 20](#_Toc121255953)

[8.5 Actions required 20](#_Toc121255954)

[9. Incident Escalation 21](#_Toc121255955)

[9.1 What attacks are taking place? 21](#_Toc121255956)

[9.2 How might this be related to stage 1? 21](#_Toc121255957)

[9.3 What would you do? 22](#_Toc121255958)

[9.4 What do you need to research before you decide? 22](#_Toc121255959)

[9.5 What has occurred? 22](#_Toc121255960)

[9.6 What impact could this have? 23](#_Toc121255961)

[9.7 Action taken to mitigate the attack 23](#_Toc121255962)

[10. Advanced Attack and Mitigations 24](#_Toc121255963)

[10.1 What Occurred 24](#_Toc121255964)

[10.2 Potential Impact 24](#_Toc121255965)

[10.3 Mitigation of Encrypted Tunnel Attacks 24](#_Toc121255966)

[10.4 Post Incident Recommendations 25](#_Toc121255967)

[10.4.1 Lessons learned: 25](#_Toc121255968)

[10.4.2 Incident Record Management 25](#_Toc121255969)

[10.5 Incident Documentation 26](#_Toc121255971)

[10.5.1 Incident Timeline Report. 26](#_Toc121255972)

[10.5.2 Information Commissioners Office (ICO) Report 26](#_Toc121255973)

[10.5.3 Police, Fraud Team and NCSC Report 26](#_Toc121255974)

[11 Recommendations 27](#_Toc121255975)

[11.1 Email 27](#_Toc121255976)

[11.2 Firewalls 27](#_Toc121255977)

[11.3 Other actions 28](#_Toc121255978)

[11.4 Invoke Disaster Recovery? 28](#_Toc121255979)

[11.5 Communications 28](#_Toc121255980)

[12 References 29](#_Toc121255981)

# 

# Introduction

Leading Edge Removals (LER) has plans to expand the business into international localities. This report will outline the recommendations to enable and support the business to achieve its aims.

Risks have been identified along with mitigation recommendations. There is a distinct lack of awareness for cyber and information security. This can leave our company exposed to data leakage, data corruption, denial of services, all may impact on our company being able to supply our customers with the excellent service they have become accustomed too. If we are hacked or services are denied to our customers our company reputation will be severely impacted and dependant on the severity, we may never recover. We do not wish to be the next Talk-Talk incident in front of the Information Commissioners Office.

# A plan for influencing the board (actions/supporting information needed/presentation)

## 2.1 Influencing the Board

A quick presentation will be shown to the board explaining the existing position, suggested improvements, and the return on sustainable investment (ROSI). In this report the risks and related vulnerabilities are conveyed, as well as what might occur if the risk is neglected and any financial penalties that might be imposed.

The simple but effective ‘Cyber Security Toolkit for Boards’ (Anonymous, 2019) is a very easy read three steps headline for our board.



Following the three steps will be the nine key requirements to help the board understand, question and comment to the solution, thus enable buy in and support of this process. (Anonymous, 2019)



Olzak, 2021 8 minute YouTube article will be the last section of the presentation. This great video gives the essential detail at high level to empower the board with effective, swift cyber knowledge. (Olzak, 2021). Just one minute into the video the Asset Owners section will identify our board responsibilities and those of our CEO, who can then allocate tasks to each department to support the company and board.

The General Data Protection Regulation (GDPR), which mandates that the information owner be accountable for the ‘protection, quality, and integrity of information’, is much easier to execute after the organisation decides the attribute, authority, and its impact. The foundation of enterprise data management is the application of predetermined strategies, tactics, and operations. Our board and senior management, are information owners, setting strategic objectives and informed decision making. (Talend, 2022)

## 2.2 Actions and Supporting Information

Identifying our assets, business criticality of those services, responsible owners of those assets, asset owners can then reduce the burden of our board. Information Asset Owners (IAO’s) will take control of their services, identify concerns, ensure access controls are commensurate with the business needs. Our board can assist this service improvement by identifying and verifying the services, criticality and owners. Our board will be asked to approve this action and formally minute the decision to show our accountability and actins approved. IOA’s can use ‘The Information Security Roles and Responsibilities’ guidance. (Anonymous, 2022)

# An assessment of the key features of ISO27001 and Cyber Essentials and their suitability for this company.

Before our company embarks on the certification road, we must identify why?

* Potential contract requirement
* Cyber maturity

If our company approves any certification scheme, the board will approve and resource the programme accordingly.

## 3.1 Cyber Essentials

In 2014 the Cyber Essentials scheme was launched with two levels of certification. The government-backed schemes enable us to improve our cyber maturity. (Anonymous, 2018). Cyber Essentials is a self-assessment certification while Cyber Essentials Plus (CE+) is independently audited. CE+ is more widely recognised as following good practice. Cyber Essentials will change as and when new threats are identified, the scheme does not permit risk acceptance as an approach.  
U.K Government requires any contractor which handles sensitive and personal information to be certified against the Cyber Essentials scheme. (Anonymous, 2018)

## 3.2 The five controls are:

### 3.2.1 Use a firewall to secure your internet connection:

The firewall acts as a gatekeeper to secure an internet connection. The firewall filters the traffic coming in and out of the network, it can block authorised access. Moreover, it can prevent your computer from getting infected by malicious software (Johansen, 2021).  
Most organisations have a boundary firewall. The people connected to the network should use a personal firewall that usually comes with the operating system (Anonymous, 2022).

### 3.2.2 Choose the most secure settings for your devices and software:

Devices are often launched with a plug-and-play model with most of the features enabled by default. Although this can enhance the user experience, it may allow potential attackers to breach your device by exploiting the vulnerabilities (Anonymous, 2022). This applies to newly installed software. Therefore, both devices and software must be configured properly to harden the level of security. For example, revoking administrative rights of Windows on an employee’s computer.

Moreover, devices including computers, mobile phones, and tablets store sensitive data of our organisation so must be protected by a strong password and encryption of data at rest.

With the secure password, an additional security layer like multi-factor authentication can be added to improve our security.

### 3.2.3 Control who has access to your data and services:

Our organisation must ensure we are protecting our user data and accounts by implementing adequate access controls, “need to know” principle. Access controls ensure that users can only see what they are permitted too. The two elements are authorisation and authentication. Authentication is a process of verifying the identity of the user while authorisation determines what a user can do once the system access has been granted (Anonymous, 2022).

### 3.2.4 Protect yourself from viruses and other malware:

We must enable protection against malware that includes computer viruses, ransomware, worms, etc. because it can lead to a major disaster such as data loss or loss of service availability.

In 2017, research by SentinelOne and Vanson Bourne found that around 40% of the organizations based in the U.K fell victim to an average of five ransomware attacks (Anonymous, 2022).

Cyber Essentials Certification requires that at least one of the approaches listed below are implemented to defend an organization from malware:

#### 3.2.4.1 Anti-malware software:

Operating systems may have built in malware protection software like Windows Defender. We must make sure the anti-malware software updated on daily basis.

#### 3.2.4.2 Application Whitelisting:

Application whitelisting process requires our system administrator to configure the computer so that it can only run specific applications.

#### 3.2.4.3 Application Sandboxing:

Application sandboxing is a process that ensures all code from untrusted sources is run within a sandbox, an isolated environment providing very limited access to the rest of your device and network.

### 3.2.5 Keep your software and devices up to date:

Devices and software are susceptible to different vulnerabilities. Therefore, it is important to install the latest updates as soon as possible when they are released. According to a recent survey by Ponemon Institute, it was revealed that almost 60% of organizations were breached due to unpatched vulnerabilities (Anonymous, 2022).

## 3.3 International Standards Organisation 27001 (ISO27001)

ISO27001 was first published in 2005. The standard has been updated regularly to keep pace with the changing cyber and information risks. ISO27001 has 114 controls which include people, technology, and process. ISO27001 is seen as a more in-depth, wider breadth security assurance than Cyber Essentials.

Our company following the implementation of Cyber Essentials Plus should consider ISO27001 for increased maturity. The ISO enables systemic considerations of information and risk management. (Anonymous, 2022)

ISO27001 is the ‘managing of information security risk’, the standard allows organisations to make business risk-based decisions with backing information on why that risk was accepted.

Consideration of the ‘Statement of Applicability’ is key with this certification. Too wide scoped, is likely to be expensive, time-consuming and our company must consider the return on investment. We must identify which service would potentially improve the company's cyber maturity, gain potential new contracts and meet any contractual requirements whilst maintaining cost-effectiveness.

## 3.4 Mandatory ISO 27001 requirements

[Scoping your ISMS](https://www.itgovernance.co.uk/blog/how-to-document-the-scope-of-your-isms) (clause 4.3), in which you define what information needs to be protected; and ensure commensurate with the information classification and criticality to the business.

Conducting a risk assessment and defining a risk treatment methodology (clause 6.12), in which you identify the threats to your information.

## 3.5 ISO 27001 mandatory clauses:

* [Information security policy and objectives](https://www.itgovernance.co.uk/blog/how-to-document-your-information-security-policy) (clauses 5.2 and 6.2)
* Information risk treatment process (clause 6.1.3)
* [Risk treatment plan](https://www.itgovernance.co.uk/blog/how-to-create-an-iso-27001-compliant-risk-treatment-plan) (clauses 6.1.3 e and 6.2)
* Risk assessment report (clause 8.2)
* [Records of training, skills, experience and qualifications](https://www.itgovernance.co.uk/blog/iso-27001-staff-awareness-training-meeting-the-requirements) (clause 7.2)
* Monitoring and measurement results (clause 9.1)
* [Internal audit programme](https://www.itgovernance.co.uk/blog/how-to-conduct-an-iso-27001-internal-audit) (clause 9.2)
* Results of internal audits (clause 9.2)
* Results of the management review (clause 9.3)
* Results of corrective actions (clause 10.1)

Annex A controls:

[Annex A](https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained) outlines the controls that are associated with various risks. Depending on the controls your organisation selects.’ (Watson, 2019)

* Definition of security roles and responsibilities (clauses A.7.1.2 and A.13.2.4)
* Inventory of assets (clause A.8.1.1)
* Acceptable use of assets (clause A.8.1.3)
* Access control policy (clause A.9.1.1)
* Operating procedures for IT management (clause A.12.1.1)
* Secure system engineering principles (clause A.14.2.5)
* Supplier security policy (clause A.15.1.1)
* Incident management procedure (clause A.16.1.5)
* Business continuity procedures (clause A.17.1.2)
* Statutory, regulatory, and contractual requirements (clause A.18.1.1)
* Logs of user activities, exceptions, and security events (clauses A.12.4.1 and A.12.4.3).

## 3.6 ISO 27001 vs Cyber Essentials:

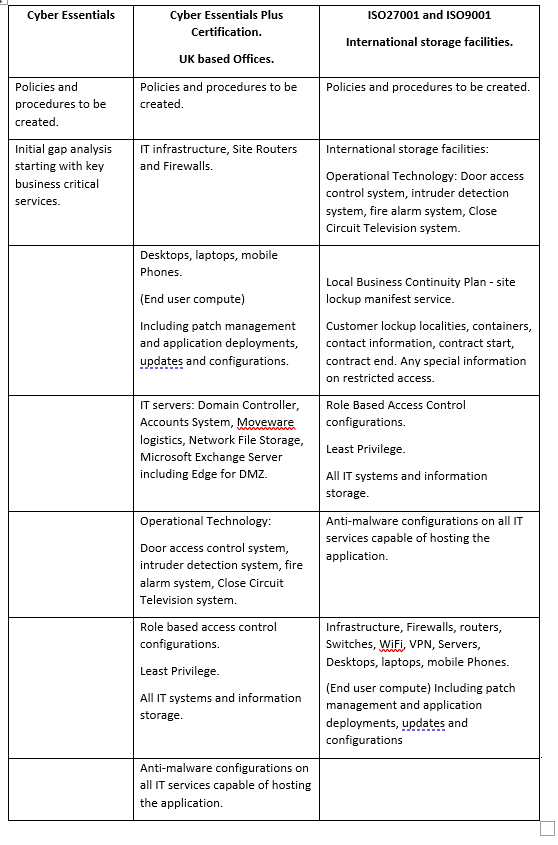
Text

Description automatically generated

REF: [ISO 27001 and the Cyber Essentials Scheme (itgovernance.co.uk)](https://www.itgovernance.co.uk/iso27001-and-the-cyber-essentials-scheme)

## 3.6 Suitability of Cyber Essentials Plus and ISO27001.

Different parts of our company may benefit from different approaches and certifications. This table gives a quick comparison guide.



Cyber Essentials Plus is not as flexible as ISO27001, as the ISO certification allows for risk management decisions, mitigations, and risk acceptance.

The Statement of Applicability (SoA) is vital to scope correctly. Too wide then the certification will become unachievable, likely unaffordable. The wording is critical to keep the focus and ensure our international customers gain the comfort and assurance of our achievement. For instance, the provision, management, 24-hour monitoring of highly professional secure storage and removals service.

# A detailed proposal for securing the company assets and developing a security culture.

## 4.1 Overview of Current Security

The main obstacle is the Security Culture in our company, but by improving the security culture we can benefit massively as employees will be more vigilante and skilled at preventing possible intrusions and attacks. A study by (Rotvold, 2007) found that a large amount of business respondents did not offer security culture training, one third of responders would like to increase their awareness, further reinforcing the importance of a competent security culture to establish and maintain a satisfactory standard.

We have limited financial and technical resources; thus, our needs must fit the revenue regardless of importance or necessity. Our company management must be looking at the minimum level of security required by law, under the Data Protection Act 2018 ((GOV.UK, 2022) and the General Data Protection Regulation ((European Union, 2018), not seeing security as a “burden”.

Furthermore, the potential cost of a breach may exceed the cost of protection implementation. The implementation can be done through hardware and software, but must also address the individual, as human error can cause data leakage. We must ensure to incorporate information security awareness into their security culture programme (Yildirim, 2016).

The “piecemeal developed” IT infrastructure that is currently in place is a security concern.

We should have one core set of servers all running supported software and the same generation of hardware to reduce the chance of vulnerabilities and compatibility issues as well as making it easier to update and manage them. At present all different ages and running different systems, will take longer and be more complicated to manage (Julia Dutton, 2021).

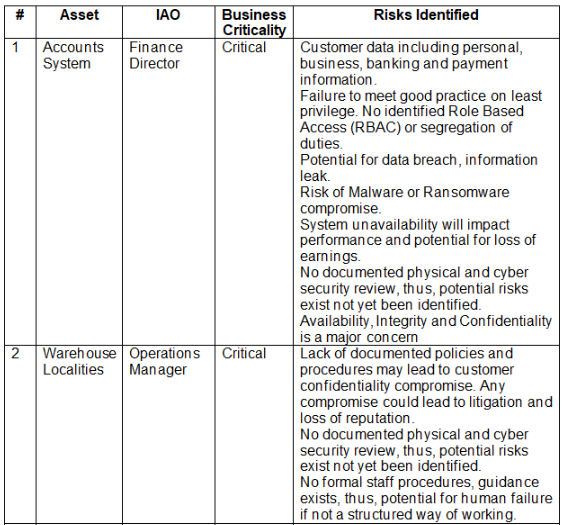
We must address the systems failures that have occurred recently that have caused significant delays in terms of work progress. Some users have fallen victim to phishing emails, downloaded viruses which is likely due to the poor security culture. Email in the company is not hosted by an ISP but it is on a server running MS Exchange in the LAN rather than DMZ, the problem being that it only stops known viruses and malware generally and is still susceptible to custom attacks slipping through systems that are not hardened (Agari, 2022).

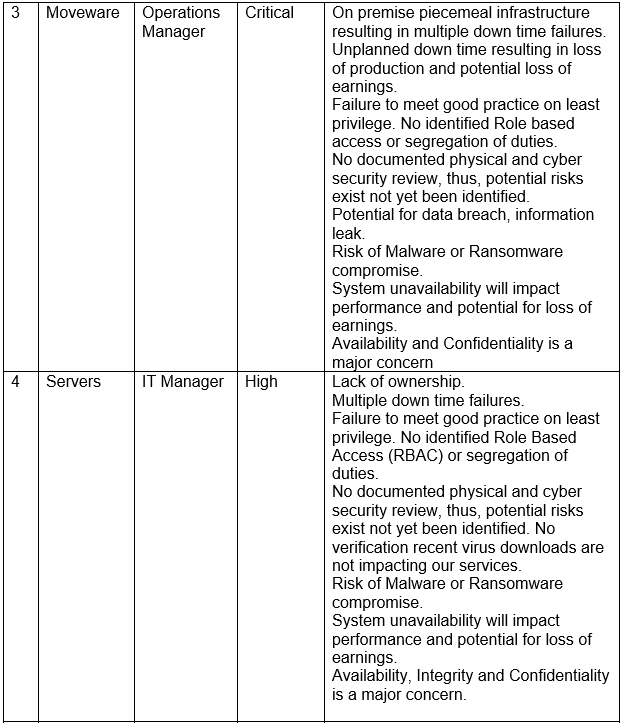
## 4.2 How Could Security be improved at the company?

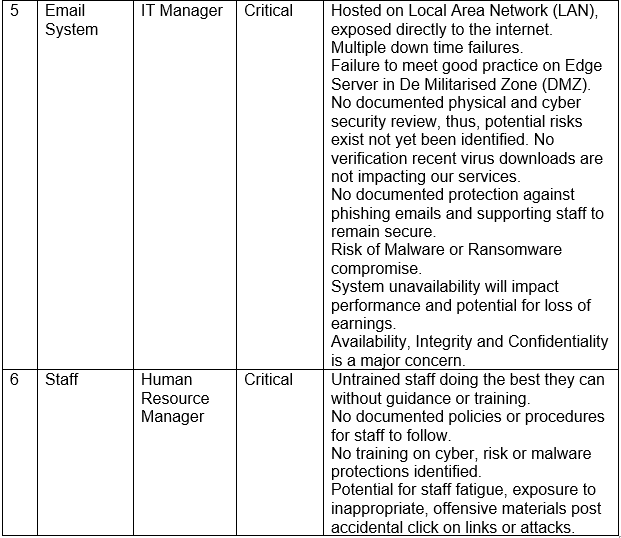
Firstly, we must become familiar with GDPR and how it can be applied within our company ((European Union, 2018). As GDPR is a regulation which enforces companies to act more carefully and responsibly when dealing with personal data of clients and employees, this is of vital importance that management and employees are aware of this regulation.

Security culture needs to be improved, which can be done though training courses provided by professionals that can outline the risks that are posed with the work forces security culture, using real-world examples of large companies that have been brought down by lax security culture. Instead of overwhelming the employees with information and lots of “don’t dos”, providing them with the basics of good security culture and trying to persuade them that they don’t want their company to be the next TalkTalk ((Information Commissioner's Office, 2015) or TK Maxx ((Simon Aughton, 2009) which both have had large breaches.

## 4.3 Risk Identification Table







### 4.3.1 Figure 1: Risk table

## 4.4 Asset Risk Matrix

Creating a plan that protects the business from its most threatening potential risks, we must first ensure we understand which risks have the highest potential of burden, a risk matrix can be used to visualise this. See figure 2.

Each asset is assessed regarding the severity of damage it could cause, as well as the likelihood of it occurring (Smith, 2009). Businesses can use the matrix to understand which risks they should address first to minimise the potential of risk, providing the company with a checklist of problems ranked by damage potential (Garvey, 1998).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Severity ->  Likelihood↓ | A. Very Low | B. Low | C. Medium | D. High | E. Very High |
| 1. Very Unlikely |  |  |  |  |  |
| 2.Unlikely |  |  | **6** | **2** |  |
| 3.Moderate |  |  |  |  | **3** |
| 4.Likely |  |  |  | **4** | **1** |
| 5.Very Likely |  |  |  | **5** |  |

### 4.4.1 Figure 2: Risk Matrix

The servers of the business have been regularly crashing. When running, it’s through a poorly optimised and piecemeal developed system. The I.T department has also failed to govern proper access rights, and data ownership, allowing connections and access to individuals in the business, where it should not be (Jäger, 2021).

The risk matrix identifies, Accounts System, Moveware, Servers and Email System are the priority for us to secure and make fit for purpose.

## 4.5 ROSI

To calculate feasibility, a ROSI can be considered, assessing an implementation worth against it’s cost. (Davis, 2005) Due to the easily accessible system, sensitive personal information could be stolen, resulting in a GDPR breach, following with a fine of €20 million or 4% global annual turnover, whichever highest. This one consequence far exceeds the costs of implementation for LER.

Furthermore, damage can be considered as delay, disruption, data leaks and data losses (Tsalis et al., 2013). These each negatively affect the business; thus, the company can assess how many of these potential damages could be minimised or eradicated, further valuing the ROSI.

# Recommendations

### 5.1 Prioritisation.

As with all services, all work packages, a logical, documented priority must be done. This will ensure the correct focus is given to the areas, ensuring efficiencies, cost effective work packages that contribute to the company aims and goals.

### 5.1.1 Instil the concept that security belongs to everyone – Risk 6.

We must develop and instil a positive security culture. To create and maintain a sustainable security culture, the entire company must be on board. Employee’s need to understand that an individual can be just as much of a solution as they can be a problem regarding security. (Rotvold, 2008)

Individuals of the business should be made aware of the dangers of email phishing, viruses, poor ownership of data, poor access rights, as well as how to spot these dangers before they occur and the best practices available to them when navigating areas of threat. An efficient example to show the breadth of these threats would be to give the individuals reports on how many viruses, spam and phishing emails come into the company. (Romeo, 2015)

### 5.1.2 Obtaining support from Senior Leadership – Risks 1–6.

Senior leadership is driven by metrics like revenue, ROI, and shareholder value. An ROI estimate for cybersecurity risk appears to be difficult to determine. However, concrete evidence of possible assaults enables management to understand the high likeliness of a breach. In a study by (Alnatheer, 2015) it was found that one of the key top factors to the critical success of security culture was top managerial support and influence for an improved security awareness and culture.

### 5.1.3 Information Technology Improvements

All Information Technology Systems will be risk assessed for defence against physical threats, Malware, Ransomware and ensure immutable backups are documented to include the restore processes. An implementation plan will be followed to reduce the risk of information extortion and exfiltration.

### 5.1.4 Accounting System – Risk 1.

Scoring the highest risk, we will enforce RBAC, enforce segregation of duties. Document all changes Improve availability thus reduce potential financial loss.

### 5.1.5 Transfer email hosting to the cloud

Currently, our email server is using MS Exchange on our LAN, this leaves too much vulnerability present to be ignored. We should instead host our email through a cloud provider. We will follow good practice as described by National Cyber Security Centre. (Anonymous, 2022)

### 5.1.6 External Threat Prevention – Risk 1,3-6.

External attacks can come in many different forms, due to this the business must have the ability to respond to a multitude of unique attacks. Firewalls, Intrusion Prevention, Access Control Lists, Security Incident Event Management system (SIEM). Dependant on costs and resources.

### 5.1.7 Servers Improvements – Risk 4

Migrate to supported common platform. Regular patching and assurance reviews will improve Confidentiality, integrity and Availability.

### 5.1.8 Moveware – Risk 3.

Migrate to cloud hosted service. Enforce RBAC. To improve Confidentiality, Integrity and Availability

### 5.1.9 Warehouse Localities – Risk 2.

Document operating procedures. Enable formal staff training.

### 5.1.10 Staff - Risk 6.

Implement positive culture training. Implement cyber security training. Notification of company policies and procedures. Support line managers with their teams and any concerns.

A Digital Solution seems the most viable solution with potentially reduced costs in the long term, as it removes the needs for a complete hardware and software upgrade which will cost a lot more upfront. A digital solution is moving the data we keep to a third-party provider cloud service and pay a subscription fee for that service.

We can reduce hardware costs, if anything needs repaired, we contact the third-party service and have them fix it which also reduces our company workload ((Amazon, 2021).

A resource if our company is considering ISO27001 certification is ‘Strongdm’ (Anonymous, 2022). The simple effective list gives a great start point in real terms.

# References:

, 2018. *Cyber Essentials Scheme: overview.* Available from: <https://www.gov.uk/government/publications/cyber-essentials-scheme-overview> [Accessed 30th October 2022].

, 2019.*Cyber Security Toolkit for Boards.*Available from: <https://www.ncsc.gov.uk/collection/board-toolkit/about-board-toolkit> [Accessed 2nd December 2022].

, 2019.*Introducing the Cyber Security Toolkit for Boards.*Available from: <https://www.ncsc.gov.uk/collection/board-toolkit> [Accessed 5th December 2022].

, 2022.*Cloud.*Available from: <https://www.ncsc.gov.uk/section/advice-guidance/all-topics?topics=Cloud&sort=date%2Bdesc> [Accessed 5th December 2022].

, 2022. *IASME Governance Self-Assessment Preparation Booklet includes assessment against Cyber Essentials and GDPR requirements.* Available from: <https://iasme.co.uk/wp-content/uploads/2022/01/IASME-governance-and-Cyber-Essentials-questions-booklet_vEvendine.pdf> [Accessed 1st November 2022].

, 2022.*Information Security Roles & Responsibilities.*Available from: <https://security.tcnj.edu/program/security-responsibilities/third-party-system-administrator-guidelines/> [Accessed 5th December 2022].

, 2022. *ISO 27001 and the Cyber Essentials Scheme.* Available from: <https://www.itgovernance.co.uk/iso27001-and-the-cyber-essentials-scheme> [Accessed 1st November 2022].

, 2022. *National Institute of Standards and Technology.* Available from: <https://www.nist.gov/> [Accessed 8th November 2022].

, 2022. *WHAT ARE THE MAIN DIFFERENCES BETWEEN CYBER ESSENTIALS, CYBER ESSENTIALS PLUS AND IASME GOVERNANCE?* Available from: <https://iasme.co.uk/cyber-blog/what-are-the-main-differences-between-cyber-essentials-cyber-essentials-plus-and-iasme-governance/> [Accessed 1st November 2022].

AGARI., 2022.*Email Security for Microsoft Exchange.*Available from: <https://www.agari.com/solutions/email-security/microsoft-exchange#:~:text=Microsoft%20Exchange%20paired%20with%20a,custom%20attacks%20slip%20right%20through.>

Alnatheer, M.A., 2015, April. Information security culture critical success factors. In *2015 12th International Conference on Information Technology-New Generations* (pp. 731-735). IEEE.

BESTPRACTICE., 2021. *What are the 14 domains of ISO 27001 .* Available from: <https://bestpractice.biz/what-are-the-14-domains-of-iso-27001/> [Accessed Oct 29th 2022].

CENTER, N. C. S., 2019. *Cyber Security Toolkit for Boards.* Available from: <https://www.ncsc.gov.uk/section/board-toolkit/home> [Accessed Oct,30].

DAVIS, A., 2005. Return on security investment – proving it's worth it*. Science Direct*. 2005 (11), pp. 8-10. Available from: <https://www.sciencedirect.com/science/article/pii/S1353485805703019?via%3Dihub.>

EUROPEAN UNION., 2018.*GDPR.*Available from: <https://gdpr.eu/> [Accessed 03/11/2022].

FRENKEN, P., 2020. *Building a Culture of Security.* Available from: <https://www.isaca.org/resources/isaca-journal/issues/2020/volume-5/building-a-culture-of-security> [Accessed 5 Nov, 2022].

GARVEY, P.R. and LANSDOWN, Z.F., 1998. Risk matrix: an approach for identifying, assessing, and ranking program risks. *Air Force Journal of Logistics*, *22*(1), pp.18-21.

GOV.UK., 2022.*Data Protection.*Available from: [https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK's%20implementation%20of,used%20fairly%2C%20lawfully%20and%20transparently](https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018%20is%20the%20UK) [Accessed 17/11/2022].

INFORMATION COMMISSIONER'S OFFICE., 2015.*TalkTalk cyber-attack – how the ICO’s investigation unfolded.*Available from: <https://ico.org.uk/about-the-ico/media-centre/talktalk-cyber-attack-how-the-ico-investigation-unfolded/> [Accessed 07/11/2022].

JAGER, A., 2021. Finding and evaluating the effects of improper access control in the Cloud.

JULIA DUTTON., 2021.*Having too many security solutions is as bad as having too few.*Available from: <https://www.vigilantsoftware.co.uk/blog/why-too-much-security-is-almost-as-bad-as-too-little-security.>

MAGNUSSON, A., 2022. *ISO 27001 Checklist: Easy-to-Follow Implementation Guide.* Available from: <https://www.strongdm.com/blog/iso-27001-checklist> [Accessed 6th November 2022].

OLZAK, T., 2021. *Information and asset ownership.* Available from: <https://www.youtube.com/watch?v=0p5L4WGY4tEabchannel> [Accessed 7 OCTUBER 2022].

ROMEO, C., 2015. *6 ways to develop a security culture from top to bottom.* Available from: <https://techbeacon.com/security/6-ways-develop-security-culture-top-bottom> [Accessed 5 Nov, 2022].

ROTVOLD, G.M., 2007. Status of Security Awareness In Business Organizations And Colleges of Business: An Analyses Of Training And Education, Policies, And Social Engineering Testing.

ROTVOLD, G., 2008. How to create a security culture in your organization: A recent study reveals the importance of assessment, incident response procedures, and social engineering testing in improving security awareness programs. *Information Management Journal*, *42*(6), pp.32-38.

SMITH, E.D., SIEFERT, W.T. and DRAIN, D., 2009. Risk matrix input data biases. *Systems Engineering*, *12*(4), pp.344-360.

SIMON AUGHTON., 2009.*TK Maxx Admits Hacker’s Theft of Data From 45.6 million Credit Cards.*Available from: <https://www.alphr.com/news/home-and-leisure/109198/tk-maxx-admits-hackers-theft-of-data-from-45-6-million-credit-cards/#:~:text=Fashion%20retailer%20TK%20Maxx%20has,to%20December%20of%20last%20year.> [Accessed 08/11/2022].

TALEND. *how to confirm data owners.* Available from: <https://www.talend.com/resources/gdpr-compliance-assigning-data-owners/> [Accessed Nov 8,2022]

TOLAH, A., FURNELL, M. S. and POPADAKI, M., 2021*. Computers & Security*. VOLUME 108 edELSEVIER.

TSALIS, N., THEOHARIDOU, M. and GRITZALIS, D., 2013, December. Return on security investment for Cloud platforms. In *2013 IEEE 5th International Conference on Cloud Computing Technology and Science* (Vol. 2, pp. 132-137). IEEE.

UCHENDU, B., NURSE, R. C., BADA, M. and FURNELL, S., 2021*. Computers And Security*. volume 109 ed

WATSON, M., 2019. *Requirements for achieving ISO 27001 certification.* Available from: <https://www.itgovernance.co.uk/blog/requirements-for-achieving-iso-27001-certification> [Accessed 1st November 2022].

YILDIRIM, E., 2016. The importance of information security awareness for the success of business enterprises. In *Advances in human factors in cybersecurity* (pp. 211-222). Springer, Cham.

Incident Response

# Introduction

A financial based company known as EdgeCoin has fell victim to a series of attacks from an unknown third party with malicious intent. The attackers have used Trojan methods of attack, meaning they have sent harmful software disguised as something else, with intent to gain access to EdgeCoin.

Using the access gained through trojan attacks, it is suspected that attackers have transferred money out of the company accounts using mule accounts as the creation date of the accounts, being the same day of the attack, has been picked up by fraud staff at EdgeCoin.

The attacks came in three stages which this report aims to assess incrementally. The report aims to assess the damage to the company in depth, as-well as suggesting actions to improve the current security issues and reduce the risk of similar incidents occurring in the future.

# Initial Event

## 8.1 Is this classified as an incident?

A security incident is an occurrence that may point to a system or data breach within an organisation or the failure of security safeguards. It includes a range of infractions, such as unauthorised access to systems, networks, and data, malware, DDoS attacks, or even the theft of actual computer hardware and devices containing critical data (Shacklett, 2022). In this case, the unknown individual is attempting to get unauthorised access to the system. Thus, qualifying as an incident.

## 8.2 Information required

Due to the nature of a Cryptocurrency business, the motivation was likely financial. The HIDS (Host-based intrusion detection system) has detected backdoor Trojan traffic block which is attempting to assert command and control (C2) on a developer PC.

To ensure that the incident is dealt with to a sufficient standard, the NIST SP 800-61 incident response life cycle (Souppaya & Scarfone, 2013) should be followed (See figure 1). This consists of four stages, the first being preparation. To ensure similar incidents do not occur again, the staff can be trained in identifying and avoid trojans, typically present through phishing emails.

Graphical user interface, application

Description automatically generated

Figure 1: Incident Response Life Cycle (Souppaya and Scarfone, 2013)

To complete the lifecycle the team must write up a report of the incident, detailing each phase of the cycle and the steps taken.

## 8.3 Likely damage to Edgecoin

Trojan refers to the attack being disguised, it does not define the threat itself, as the attack can be incredibly versatile for the needs of the attacker (Zhenfang, 2015).

Successful attackers could attempt to empty customer’s cryptocurrency wallet into their own (Boireau, 2018), or a proxy wallet on the (C2) as well as customer’s personal finances (Granger, 2001). Furthermore, personal sensitive information could be stolen, constituting a breach of GDPR (Seo et al., 2017).

Reputational damage could be the biggest threat from this attack (Sinanai and Muntermann, 2013).

The attacker can also attempt to execute commands to the developer PC to disrupt or potentially stop system processes. (Malik et al., 2021).

## 8.4 Future risk if not resolved

If news gets out we may suffer reputational damage. New customers will be hard to attract as they will not feel their money is secure. Loss of data can potentially lead to ransom demands from the attacker.

The possibility of downtime due to the attack means a loss of revenue in terms of customer trading and the system’s repair.

Edgecoin could be liable to fines from customers suing the organisation. A DDOS attack in 2011 resulted in a £250,000 fine for Sony, due to a ‘serious breach of the data protection act. (Osborne, 2014)

## 8.5 Actions required

Improper communication can impact the business efficiency, interviews may need to take place to gather evidence, as described by (Cichonski et al., 2012) and (Dittrich and Dietrich, 2008).

Remote forensics’ capability, conducting an analysis to gain insight into how the attack operated (Case and Richard, 2017).

This analysis may assist Edgecoin in the detection, containment, and eradication of the threat (Ligh et al., 2014), two of the Incident Response Life Cycle stages. (Eden et al., 2015). This is discussed further in section 5.

# Incident Escalation

## 9.1 What attacks are taking place?

We have been breached as the attackers have gained access to our finances and they are using Mule accounts to transfer money from our accounts. The breach could have happened through several popular methods (Melnick, 2022), the most likely being listed below:

* Phishing (Trojan virus)
* Company Information purchased on the dark web
* Brute force attack
* Dictionary attack
* Tunnelling attack

It is clear however, based on the evidence collected and from what can be surmised, the company fell victim to a Tunnelling attack ((C&S Specialty Underwriters, 2021) which could have led to the attacker gathering enough information to gain access to the company's financial information.

## 9.2 How might this be related to stage 1?

Stage one seems to be the initial warning sign of an incoming attack or a breach in the system. There were several alerts for backdoor Trojan traffic from the HIDS (Host-based Intrusion Detection System) on a remote developer’s computer, which was reported though the SIEM (Security Information and Event Management) system.

The Trojan virus may have been attached to a file or document that was then downloaded or accessed by the target user and in most circumstances, it is well hidden and may appear with the face of other software or hide inside the files of a seemingly legitimate file or download (Jaiswal, 2017).

It can be surmised that stage one of the attack was indeed the trojan traffic that was detected in the system and then DNS tunnelling was used to exfiltrate the financial data which was then used by the hacker to gain access to the company finances and make deposits from the company accounts to their own mule accounts.

## 9.3 What would you do?

There are several steps that need to be taken in order to secure the company network and stop any further damage to the company and its assets. Several generalised steps that need to be taken are listed below in order of priority:

1. Quarantine of the original compromised device and user.
2. All access should be cut-off for the hacker, and this can be done by creating a one-way traffic of data, instead of sending and receiving, company financials should be set-up to only receive.
3. Finding and removing malicious software
4. Reinforcement of security protocols and procedures

## 9.4 What do you need to research before you decide?

To form a swift and effective response plan of action, research needs to be conducted into the following areas:

* Are there any current response procedures in place at the company?
* If yes, are the response procedures sufficient?
* Isolation and removal of malicious software
* Reinforcing security protocols and procedures

## 9.5 What has occurred?

In summary, we have been breached through a tunnelling attack in which an employee most likely fell victim to a phishing attack that planted a trojan on the system and allowed the hacker to gain access to the company’s financial information.

The HID system issued a significant number of alerts that suggested backdoor Trojan traffic and additionally the third-party firewall provider detected UDP attack traffic and recommended that the company start attack mitigation procedures.

The company’s accounts have also had deposits being made to multiple mule accounts which are suspected to be owned by the hacker.

## 9.6 What impact could this have?

An unidentified malicious party has gained access to EdgeCoin’s systems, managed to get beyond all security measures, and created several mule accounts to transfer money between different accounts.

The trojan attack has had a significant negative impact on EdgeCoin since it has made it impossible for users to access the services that are offered by EdgeCoin. As a result, many users were unable to perform the routine tasks that they expect the system to perform for them. EdgeCoin's possible long-term impacts are unknown currently, although trojan attacks affect EdgeCoin in some way:

* Remediation Costs
* Loss of Revenue
* Damage to Reputation
* Loss of Productivity

## 9.7 Action taken to mitigate the attack

In order to mitigate and attempt to prevent these types of breaches in the future there are several steps that need to be taken by the company, listed below in no order:

* Improve overall Security Culture of the Company
* Ensuring employee access to resources are suitably restricted
* Intensive and regular network traffic monitoring
* Rigorous user access management controls

# Advanced Attack and Mitigations

## 10.1 What Occurred

Discussions with 3rd party network security providers show that Edge Coin’s network has multiple active SSL tunnels constantly exfiltrating a large amount of data that are also consuming high bandwidth.

Since the development work of Edge Coin is done remotely by connecting to the company’s VPN and it has also been observed that one of the developers' computers is raising alarms for a backdoor trojan traffic block, the attacker has likely used site-to-site tunnels after compromising the initial system. This type of attack can usually go undetected because inspecting site-to-site is rare due to the impact on the performance (Carter, 2021).

Another possible attack could be using SSH Tunnels to move payloads. SSH allows a client to connect to the server securely by authenticating using private keys often referred to as SSH keys. These SSH keys are of high interest to the attackers considering that they provide administrative access to a server. SSH Tunnels are often used to exfiltrate data from a server and since the connection is secure, it can go undetected as copying files is a normal routine (Carter, 2021).

## 10.2 Potential Impact

The impact of encrypted tunnels could be huge as these types of attacks are hard to detect. The attackers could potentially install malware like ransomware that could end up locking up the data stored on the computers connected to the network and asking for financial payment. The fact that Edge Coin is a financial organization that stores highly sensitive data of the customers, the attackers could steal personal details and wallet information. In 2017, a report showed that a similar encrypted tunnel attack against Yahoo caused a huge data breach between 2013 and 2014 costing the company around $350 million (Hernandez, 2022).

## 10.3 Mitigation of Encrypted Tunnel Attacks

According to a study from A10 Networks, it was found that around 41% of cyber-attacks use encryption to evade detection. Despite this, a survey by Venafi in 2017 found that 23% of security professionals were unaware of how much of their encrypted traffic is decrypted and inspected (Anderson, 2018).

Although protection against encrypted tunnels can be challenging, the most effective way to prevent this is to implement an SSL/TLS decryption system that provides enhanced visibility of the data streams. However, this system can only decrypt traffic if you have access to the private keys of all the systems being monitored. (Carter, 2021).

It is also important to keep decryption systems up to date as the certificates get expired and are renewed. The amount of decrypted traffic may get decreased if the certificates are not kept up to date which can eventually lead to security loopholes (Anderson, 2018).

Lastly, the process of keeping the certificates and private keys should be automated as it is not practical for our organisation to do it manually. There are many tools available that can be integrated with the organization network providing SSL decryption, next-generation firewalls, intrusion prevention and much more.

## 10.4 Post Incident Recommendations

### 10.4.1 Lessons learned:

A vital part of any incident is to learn and improve from any incident, even if the incident is a test, desktop exercise or event. Lessons learned are best done when the incident is fresh in our minds, we should start within 72 hours post the incident resolution is declared. This is an adaptation of the NIST 800-63 example. (Cichonski et al., 2012)

### 10.4.2 Incident Record Management

Our records management of the incident is crucial. We must document events, decisions, and outcomes both successes and failures. This will be used to learn for future incidents and ensure we have a complete chain of custody including decision logs and outcomes for internal, external or third-party review. The use of a nominated scribe who is not involved with the technical incident response, or resolution implementation, is strongly advised. This enables the specialists to focus on triage, resolution and designs and not lose focus updating the incident response log or communications templates. For this incident, we used a dedicated scribe and stored all records on our corporate record management system.



## Incident Documentation

### 10.5.1 Incident Timeline Report.

This is probably the most important document throughout an incident. This document will be archived for historical purposes and may also be used for potential legal action. As a minimum the initial incident must contain:

* Date
* Time
* Location
* Type of incident
* How discovered
* Contact name
* Contact number

### 10.5.2 Information Commissioners Office (ICO) Report

As per the ICO guidance because this incident impacted customers data, customers finance we must report this to the ICO within 24 hours of discovery. (Anonymous, 2022).

### 10.5.3 Police, Fraud Team and NCSC Report

As our service has been compromised and payments extracted from customer accounts we must inform the fraud team, police and NCSC so they can link any previous, ongoing attacks to assist all parties. The incident timeline report will be sufficient.

# Recommendations

The following recommendations will help reduce risk, mitigate similar attacks and enable a more secure and available service.

## 11.1 Email

We will review the 3rd party configuration of our hosted email service As SPAM emails and fake delivery receipts have been identified. The correctly configured, Sender Policy Framework (SPF), Domain Keys Identified Email (DKIM) and Domain-based Method Authentication Reporting and Conformance (DMARC) protocols are designed to reduce such attacks. The ‘Email Authentication Best Practices’ EasyDMARC (Anonymous, 2022) and ‘Email security and anti-spoofing’ NCSC (Anonymous, 2019) recommendations show how we can secure our email service and reduce spoof attacks claiming to be from us to our customers. Especially using the forced check SPF setting ‘-all’, as any non-authenticated email will be rejected by the remote users as SPAM.

We will work on the email security gateway, verify patched to latest levels. Ensure anti-malware and anti-phishing software is up to date and correctly configured.

## Firewalls

Ensure security in depth with multi-layer firewalls. All firewalls up to latest patching and review configurations for improvements such as:

* Configure Intrusion prevention Service with automated rules enabled. If one of our devices is confirmed infected, that device will be quarantined from our services automatically.
* Web Application Firewalls will be configured to good practice as per Cloudflare and Imperva recommendations, both identify key requirements and potential customer failings. (Anonymous, 2022), (Dickerson, 2020).
* Network Access Control (NAC, NACL) configuration following good practice to only permit known good traffic between services, users and network segments. This aligned with network Segmentation will enhance our security posture. (Risk, 2021).
* Terminate suspicious traffic including large data exfiltration and suspected command and control services.

## 11.3 Other actions

* Creation of new wallet/payment accounts will be verified by a second human before any payments are made.
* Review the Edgecoin service accounts for suspicious, recently created accounts that have no clear business need, these accounts should be locked and a secondary review to ascertain if they are genuine or not.
* Creation of new Policies, Procedures, Plans and Guidance for our company.
* Cyber training and awareness for staff.
* Specialist training for the incident team. (Exercise incidents such as desktop scenarios to give staff confidence.)
* Enable an immutable backup and restore solution with documented procedure.
* Test backups and restores for critical services.
* Implement cost effective vulnerability scanning external services, if funding permits then internal. Including regular reports for IT and the board.
* Patch management procedure and reporting of all services.
* Complete risk assurance of critical services.
* Create real-time alerting and escalation procedures for our key services.
* Create Business Continuity Plan
* Create Disaster Recovery Plan.

## 11.4 Invoke Disaster Recovery?

Risk assesses the invocation of the DR service vs terminate suspicious destinations plan, to ensure we have a stable, secure service and do not miss any legitimate customer transactions.

## 11.5 Communications

Communicate (anonymously) with Cyber Security Information Sharing Partnership (CISP)and other specialist services to see if they have any advice, suggestions or aware of any similar attacks and mitigations taken.

# References

, 2022. DMARC, DKIM, SPF: Email Authentication Best Practices. Available from: <https://easydmarc.com/blog/dmarc-dkim-spf-email-authentication-best-practices/> [Accessed 5th December 2022].

, 2019. Email security and anti-spoofing. Available from: <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/recommended-implementation-plan> [Accessed 5th December 2022].

, 2022. Report A Breach. Available from: <https://ico.org.uk/for-organisations/guide-to-eidas/breach-reporting/#:~:text=At%20a%20glance%201%20If%20a%20security%20breach,to%20inform%20the%20wider%20public%20about%20a%20breach.> [Accessed 5th December 2022].

, 2022. Web Application Firewall explained. Available from: <https://www.cloudflare.com/en-gb/learning/ddos/glossary/web-application-firewall-waf/> [Accessed 5th December 2022].

ANDERSON, T., 2018. Four steps organisations can take to protect against encrypted tunnel attacks . Available from: https://securitybrief.co.nz/story/four-steps-organisations-can-take-protect-against-encrypted-tunnel-attacks [Accessed 29 November, 2022].

BOIREAU, O., 2018. Securing the blockchain against hackers. Network Security, 2018(1), pp.8-11.

CARTER, S., 2021. The 5 Worst Things Attackers Can Do in Your Encrypted Tunnels. Available from: https://www.venafi.com/blog/5-worst-things-attackers-can-do-your-encrypted-tunnels [Accessed 28 November, 2022].

CASE, A. AND RICHARD, G.G. (2017) “Memory forensics: The path forward,” Digital Investigation, 20, pp. 23–33. Available at: <https://doi.org/10.1016/j.diin.2016.12.004>.

CICHONSKI, P., MILLAR, T., GRANCE, T. AND SCARFONE, K., 2012. Computer security incident handling guide. NIST Special Publication, 800(61), pp.1-147.

CICHONSKI, P., MILLAR, T., GRANCE, T. and SCARFONE, K., 2012. Computer Security  
Incident Handling Guide. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf> [Accessed 22nd Nov 2022].

C&S SPECIALTY UNDERWRITERS., 2021.*How hackers gain access to your company’s accounts — and how to stop them.*Available from: <https://csunderwriters.com/how-hackers-gain-access-to-your-companys-accounts-and-how-to-stop-them/> [Accessed 05/12/2022].

DICKERSON, S., 2020. Best Practice for Defense in Depth. Available from: <https://www.imperva.com/blog/waf-and-rasp-best-practice-for-defense-in-depth/> [Accessed 5th December 2022].

DITTRICH, D. AND DIETRICH, S. (2008) “P2P as botnet command and control: A deeper insight,”2008 3rd International Conference on Malicious and Unwanted Software (MALWARE) [Preprint]. Available at: <https://doi.org/10.1109/malware.2008.4690856>.

EDEN, P., BLYTH, A., BURNAP, P., CHERDANTSEVA, Y., JONES, K. AND SOULSBY, H., 2015, September. A forensic taxonomy of SCADA systems and approach to incident response. In 3rd International Symposium for ICS & SCADA Cyber Security Research 2015 (ICS-CSR 2015) 3 (pp. 42-51).

GEPP, K., SANTOS-LANGHURST, A. and RAYPOLE, C., 2022. How to Treat and Prevent Mental Exhaustion. Available from: <https://www.healthline.com/health/mental-exhaustion> [Accessed 1st December 2022].

GRANGER, S., 2001. Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18.

HERNANDEZ, A., 2022. Cost of a Machine Identity Data Breach with Yahoo! . Available from: <https://www.venafi.com/blog/cost-machine-identity-data-breach-yahoo> [Accessed 29 November, 2022].

HILDEBRAND, C., 2021. DDoS by the Numbers. Available from: <https://www.netscout.com/blog/asert/our-new-ddos-normal-isnt-all-normal> [Accessed Nov 6, 2022].

JAISWAL, M., 2017. COMPUTER VIRUSES: PRINCIPLES OF  
EXERTION, OCCURRENCE AND AWARENESS*. International Journal of Creative Research Thoughts (IJCRT) 2017*. 5 (4), pp. 2. Available from: <https://deliverypdf.ssrn.com/delivery.php?ID=762127125113124112109092026081079092121071009035059050117015111000078120109029080126050101098044042040042066111125076077089095104038000060086102103097071116123081005023050081020016125005121010006005106001088005014113119102118107125066104070065104122105&EXT=pdf&INDEX=TRUE.>

LIGH, M.H., CASE, A., LEVY, J. AND WALTERS, A., 2014. The art of memory forensics: detecting malware and threats in windows, linux, and Mac memory. John Wiley & Sons.

LTD, A., 2022. What is the objective of Annex A.16.1 of ISO 27001:2013? Available from: <https://www.isms.online/iso-27001/annex-a-16-information-security-incident-management/> [Accessed 2 Dec, 2022].

MALIK, A.W., ANWAR, Z. AND RAHMAN, A.U., 2022. A novel framework for studying the business impact of ransomware on connected vehicles. IEEE Internet of Things Journal.

MELNICK, J., 2022.*Top 10 Most Common Types of Cyber Attacks.*Available from: Top 10 Most Common Types of Cyber Attacks (netwrix.com) [Accessed 04/12/2022].

OSBORNE, C., 2014. Sony PlayStation Network struck by DDoS attack, bomb threat grounds executive. Available from: [https://www.zdnet.com/article/sony-playstation-network-struck-by-ddos-attack-bomb-threat-grounds-executive/.](https://www.zdnet.com/article/sony-playstation-network-struck-by-ddos-attack-bomb-threat-grounds-executive/)

RISK, E., 2021. Access Control Lists (ACLs): How They Work & Best Practices. Available from: <https://www.twingate.com/blog/access-control-list/> [Accessed 5th December 2022].

SEO, J., KIM, K., PARK, M., PARK, M. AND LEE, K., 2017, October. An analysis of economic impact on IoT under GDPR. In 2017 International Conference on Information and Communication Technology Convergence (ICTC) (pp. 879-881). IEEE.

SOUPPAYA, M. and SCARFONE, K., 2013. Guide to Malware Incident  
Prevention and Handling for  
Desktops and Laptops*. NIST Special Publication 800-83 Revision 1*, pp. 15-19. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.>

SHACKLETT, M. E., 2022. What is a security incident? Available from: <https://www.techtarget.com/whatis/definition/security-incident> [Accessed 2 Dec, 2022].

SINANAJ, G. AND MUNTERMANN, J., 2013. Assessing corporate reputational damage of data breaches: an empirical analysis.

SUNDT, C., 2006. Information security and the law. Information Security Technical Report, 11(1), pp.2-9.

ZHENFANG, Z.H.U., 2015. Study on computer Trojan horse virus and its prevention. International Journal of Engineering and Applied Sciences, 2(8), p.257840.