Intellectual property and information security: sensible foundations for micro and small enterprises

Jonathan Rhodes

Haaga-Helia University of Applied Sciences
Bachelor of Business Administration
Thesis report
2023

Abstract

Author(s)
Jonathan Rhodes

Degree
Bachelor of Business Administration

Report/Thesis Title
Intellectual property and information security: sensible foundations for micro and small enterprises

Number of pages and appendix pages
70 + 1

Protecting the intellectual assets of a small business can be a daunting task for a business manager, considering the multitude of information security threats.

This report describes the means of protecting intellectual assets and provides a checklist of measures that a manager of a micro or small enterprise could reasonably take to keep their intellectual assets secure.

The report covers a case study of poor security, legal protection through registration and protections for trade secrets, legal recourse in the event of infringements, physical and structural security in buildings, organisational measures, software security, hardware security, network security and cloud security.

As a “product” of the report, the appendices include a security cube, with six categories of security points in the form of a checklist on each face of the cube.

Key words
Information security, legal protection, software security, hardware security, network security

Table of contents

1 Introduction

This report seeks to describe the means by which a micro or small enterprise could protect its intellectual property. This report uses Eurostat’s definition of micro and small enterprises as follows:

- **micro enterprises**: less than 10 persons employed
- **small enterprises**: 10-49 persons employed (Eurostat, 2023)

Micro and small enterprises are chosen as the target group because prior research has shown that organisations of these sizes are less likely to deploy information security protections than larger organisations (Johns, 2021).

The research is conducted from the perspective of the person responsible for intellectual property in a micro or small business and seeks to answer the following key question:

What do I need to do to keep my company’s intellectual assets safe?

This question is very broad-ranging. Therefore, I break it down into seven different aspects of security, leading to the following sub-questions:

1. What legal protections are available for intellectual assets?
2. How can intellectual assets be physically protected in buildings?
3. How can organisational measures protect intellectual assets?
4. What action can be taken to ensure software security?
5. What action can be taken to ensure hardware security?
6. What can be done to secure networks?
7. What security measures are required in the cloud?

The overlay matrix in Table 1 shows the links between the investigative questions and the sections of this report.

Table 1. Overlay matrix

Investigative questions	Theoretical framework (chapter)	Results (chapter)
• What legal protections are available for intellectual assets?	4	11.1
• How can intellectual assets be physically protected in buildings?	5	11.2

• How can organisational measures protect intellectual assets?	6	11.3
• What action can be taken to ensure software security?	7	11.4
• What action can be taken to ensure hardware security?	8	11.5
• What can be done to secure networks?	9	11.6
• What security measures are required in the cloud?	10	11.7

Central to the analysis of which security measures are appropriate for a micro or small enterprise is the issue of resource expenditure. As mentioned above, micro and small enterprises have more limited resources for security investments, so the report recommends relatively inexpensive actions.

The report presents answers to these questions in the form of a security checklist. It also produces a “security cube” – a six-faceted checklist that can conveniently sit on a business manager’s desk to remind them of the importance of protecting intellectual assets among their many other duties.

The research is conducted by collecting information from authoritative sources in each area, analysing the information and presenting findings that are relevant in the context of a micro or small enterprise. The authoritative sources include academic literature, standards (such as ISO), legislation and academic analysis of legislation, and technical documentation from the providers of industry-standard solutions, including Microsoft, Google and AWS. The objective is to bring together best practices from the sources into a form applicable to a small business. Finally, the report addresses the research question stated above by producing a checklist of essential measures for small businesses to consider.

Where possible, the research is based on the latest information available at the time of writing (spring 2023) to avoid recommending outdated techniques. For this reason, the research makes extensive use of product and service documentation from the dominant service providers of the time.

Naturally, the measures applicable to any individual company will be highly dependent on the nature of that company’s business. To this end, the report seeks to identify cases where certain measures could be more or less appropriate. For example, one company may choose to register all its intellectual property with the public authorities, while another may prefer to keep such information secret.

This research method was chosen because it draws on academic and official sources to provide tangible information that a business owner or manager could put into practice in today’s operating environment.

2 Theoretical framework

2.1 Background

Intellectual property rights are increasingly the cornerstones of innovative businesses. In Europe and the USA, intangible assets account for a vastly larger proportion of market value than tangible ones since at least 2015 (Ocean Tomo, 2020). Even companies whose value is primarily based on tangible goods often augment the value of such goods by integrating them with intangible assets, such as brands and technologies (Moberly, 2014). In a knowledge-based economy, enterprises must retain the exclusive ability to exploit their intangible intellectual assets and capture the associated value to achieve consistent competitive advantage (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2013). Exclusivity is even more important in the transition to a data-based economy, where companies may possess stores of highly valuable information on their clients, industries and competitors. Such information may be difficult to place a value on, more so than assets such as patents and brands (Almeling, Snyder, Sapoznikow, McCollum, & Weader, 2009).

Intellectual property can come under threat in a wide variety of ways. Research by the Economist Intelligence Unit found that firms were most worried about losing control of trade secrets due to cybersecurity weaknesses, leaks by employees and third parties, competitive intelligence and corporate (industrial) espionage. (The Economist Intelligence Unit, 2021) The costs of the theft of intellectual assets may be very high: research has estimated the cost of trade secret theft at 1 to 3 per cent of GDP in advanced countries (Passman, Subramanian, & Prokop, 2014). The principal risk to enterprises in the event of the disclosure of trade secrets is a loss of competitive advantage: for example, if the source code to software such as Adobe Photoshop became public, cheaper (or even free) substitutes would spring up quickly. This, in turn, would chip away at the lucrative monthly revenues that Adobe is currently able to collect for its software.

With such a diverse threat landscape, a company may need to implement a broad palette of measures to protect its intellectual assets. The protections available range from registration with the authorities to technical and contractual measures to prevent the disclosure of unregistered trade secrets. While large enterprises may have greater resources for innovation and the protection of intellectual assets (OECD, 2018), it may be less feasible for small businesses to use complex methods of protection (Olander, Hurmelinna, & Mähönen, 2009). Therefore, it would be useful for small businesses to have access to a list of recommendations for keeping their intellectual assets secure.

This topic can be approached from a number of angles. With regard to the legal protections afforded to trade secrets, the applicable legal framework for a business operating in Finland are the WTO agreements, EU Directives and the implementing national legislation. In addition, legal literature analyses the application of legal and regulatory protections.

As far as information security management is concerned, the ISO/IEC 27000 family provides a standards ecosystem for managing information security and data protection in organisations. The parent standard is ISO/IEC 27001, which covers a broad range of best practices for establishing an Information Security Management System (ISMS). It was last updated in October 2022 to include recommendations for modern business practices, such as Bring Your Own Device (BYOD), working remotely and the fourth industrial revolution (Industry 4.0) (The British Standards Insitution, 2023).

The ISO/IEC 27001 standard sets out generic requirements that are intended to apply to all types organisations, large or small (International Organization for Standardization, 2022). Consequently, the standard includes many higher-level requirements in areas such as auditing and reporting that may not be among the top priorities of a small company looking to secure its intellectual property.

However, the various other standards in the ISO/IEC 27000 family delve into more detail on the specifics of information security and data protection in the following areas, among others:

- Telecommunications (ISO/IEC 27011)
- Cloud services (ISO/IEC 27017 and ISO/IEC 27018)
- Cybersecurity (ISO/IEC 27032)
- Network security (ISO/IEC 27033)
- Application security (ISO/IEC 27034)

In addition, the ecosystem contains standards on matters such as incident management and auditing. While these aspects are valuable from an organisational development standpoint, they do not directly address the primary concern of this report, which is to prevent intellectual property from falling into the wrong hands.

Microsoft has released information security advice such as ten tips for protecting files on PCs and in the cloud (Diamond, 2020). While the advice is sound in principle, it is geared towards Microsoft products.

In a similar vein, the US Federal Communications Commission publishes a list of 10 cybersecurity tips for small business (Federal Communications Commission, 2023) and links to cybersecurity resources.

The Global Cyber Alliance provides a Cybersecurity Toolkit for Small Businesses, which provides some advice on best practices in condensed format (the handbook runs to 24 pages). This is a reader-friendly text with straightforward advice explained clearly. It is an excellent source of basic advice, although it does not provide any actionable information related to cloud environments or network security (Global Cyber Alliance, 2023).

2.2 Threat landscape

This section examines the threats facing small businesses if their intellectual assets are stolen.

Businesses in the knowledge economy must strike a delicate balance between ensuring the secrecy of their intellectual property and facilitating sufficient access to the same information to enable their employees to work productively. The coronavirus pandemic increased the proportion of employees who usually work from home (i.e., for more than 50 per cent of their working time) by 8.0 percentage points across the EU on average. In 2021, over 35 per cent of employees in the Helsinki-Uusimaa region usually worked from home (Eurostat, 2022). Studies have found that working from home is likely to persist following the apparent end of the pandemic (Smite, Moe, Hildrum, Gonzalez-Huerta, & Mendez, 2023), so organisations must also ensure the security of their intellectual assets in remote-working settings.

In addition, the field of malicious actors is expanding with the advent of Crime as a Service (CaaS). CaaS is a business model where cybercriminals, malware developers and other malicious actors provide customers with access to hacker-level malware in return for a fixed fee or, depending on the service, a percentage of the money extorted. The transactions are carried out in cryptocurrencies to preserve the anonymity of the parties involved. (Schwartz, 2016)

The products available include:

- Ransomware as a Service
- DDos on demand
- PCs with preinstalled malware
- Bitcoin “tumbling”, a form of money laundering of the cryptocurrency
- Phishing kits
- Malware kits (Unni, 2022; Schwartz, 2016)

The difficulty for legitimate businesses and law enforcement agencies are that CaaS perpetrators and customers can easily remain anonymous and their financial transactions are difficult to trace. CaaS is a lucrative business with little chance of arrest. The business model is so refined that some CaaS actors have established “customer care centres” to advise victims on how to obtain bitcoins for the payment of ransoms to decrypt their data. (Schwartz, 2016)

European businesses report fearing cybercrime perpetrated by competitors, hacktivists and foreign state-sponsored attacks (PricewaterhouseCoopers, 2019).

According to PricewaterhouseCoopers, the impacts of these threats on businesses are many, including:

- Opportunity costs
- Lost sales or lost first-mover advantage
- Loss of the value of research and development
- Money invested into research and development does not provide substantial competitive advantage if the outcomes of the research and development are freely available to other parties
- Higher security costs
- More money must be invested in security to combat digital threats, resulting in less money available for other uses
- Reputational harm
- Companies could lose the trust of customers and partners if it comes to light that they have been subjected to a data breach (PricewaterhouseCoopers, 2019)

3 Case study – Uber

3.1 Introduction

Uber offers a cautionary tale for small businesses. Although Uber is by no means a small business itself, it has suffered information security breaches of types that could affect a company of any size. Some of the security failings described below could be readily rectified by following modern standards from the outset, as a company of any sized should be advised to do.

3.2 A history of breaches

The ridesharing company Uber has suffered numerous data breaches.

In May 2014, hackers gained access to Uber resources exposing the personal data of approximately 50,000 consumers (United States Attorney's Office, 2022). The data was accessed using credentials stored in plaintext in Uber’s GitHub repository, and the attacker used the credentials to access an AWS S3 bucket. The Federal Trade Commission issued a complaint to Uber admonishing it for several security failings, including storing sensitive personal information about customers and drivers in plaintext in the S3 bucket and failing to use multifactor authentication (Clark, 2017).

In September 2022, Uber revealed that an intruder believed to be from the Lapsus$ hacking group had gained access to “several internal systems”, as well as tools such as G-Suite and Slack. The systems were accessed using a compromised account belonging to an external contractor. The account required two-factor login, which the attacker was able to circumvent by persisting in sending login requests until the account owner eventually accepted one. Uber revealed that the attacker was able to access all the company’s vulnerability reports at HackerOne, a cybersecurity company. (Uber, 2022) The loss of this data potentially exposes Uber to new security risks. Beyond that, however, it is currently unclear whether any other intellectual assets belonging to Uber were stolen in the 2022 data breach.

However, at the time of writing, the data breach with the most far-reaching ramifications for Uber was the one that occurred in 2016.

3.3 The 2016 Uber data breach

In November 2017, Uber CEO Dara Khosrowshahi announced that Uber had suffered a data breach in “late 2016” (Khosrowshahi, 2017), a timeframe narrowed down to October 2016 in a subsequent Uber release (Uber, 2023). The company had kept the data breach under wraps for more than a year.

The 2016 data breach was perpetrated by two attackers (Khosrowshahi, 2017) via GitHub. According to an analysis by the US Federal Trade Commission (Federal Trade Commission, 2018), Uber's engineers were allowed to access Uber's GitHub repositories via their individual GitHub accounts, set up with personal email addresses. The intruders gained access to Uber's GitHub repository by exploiting credentials exposed in other large data breaches.

Once the attackers had gained access to the GitHub repository, they discovered an AWS access key, which they used to download files from Uber's AWS S3 bucket. The files contained the following personal data about riders and drivers in the US:

- 25.6 million names and email addresses
- 22.1 million names and mobile phone numbers
- 607,000 names and driver's licence numbers

Uber subsequently reported that about 30,000 riders and drivers in Finland were affected (Uber, 2023). The files downloaded from S3 were not encrypted (Federal Trade Commission, 2018).

In November 2016, one of the attackers contacted Uber to demand a "six-figure payout" (Federal Trade Commission, 2018). Joseph Sullivan, then Chief Security Officer at Uber, verified the accuracy of the attacker's claims and agreed to pay $100,000 in Bitcoin via the third-party company in charge of Uber's bug bounty programme (United States Attorney's Office, 2022; Federal Trade Commission, 2018). Bug bounty programmes are usually aimed towards "white-hat hackers": people who report bugs and security vulnerabilities to software developers in return for a financial reward, without exploiting the bug or vulnerability for personal gain. This practice enables the bug or vulnerability to be fixed before it becomes more widely known and is exploited in the wild. However, the perpetrators of the 2016 data breach could not be considered white-hat hackers, as they had exploited the vulnerability to download sensitive data.

Sullivan agreed on the payout on the condition that the hackers sign non-disclosure agreements in which they promised to keep quiet about the hack. Uber made the payout even though the hackers refused to reveal their true identities. When Uber succeeded in identifying the hackers in January 2017, Sullivan arranged for them to sign new non-disclosure agreements in their true names (United States Attorney's Office, 2022).

The Federal Trade Commission notes that at the time of the 2016 data breach, the Commission was already investigating Uber for the security practices surrounding its 2014 data breach, which also involved the loss of sensitive data from an S3 bucket via credentials stored on GitHub (Federal Trade Commission, 2018).

According to the United States Attorney’s Office, Sullivan went to great lengths to cover up Uber’s internal investigation of the security breach and prevent the Federal Trade Commission from finding out about it. Within Uber, Sullivan continued to work with the company’s lawyers, including its General Counsel, to address matters arising from the Federal Trade Commission’s inquiry into the 2014 data breach. Throughout this, Sullivan did not mention the new (2016) data breach. (United States Attorney's Office, 2022)

Sullivan was involved in further efforts to cover up details of the 2016 data breach from colleagues, including Uber’s CEO, and external parties, such as lawyers investigating the incident. Ultimately, Uber publicly disclosed the 2016 data breach more than a year after the fact, in November 2017. The two hackers identified by Uber were prosecuted and pleaded guilty to their charges in October 2019. In October 2022, Sullivan was convicted of obstructing the Federal Trade Commission and concealing knowledge of a felony by attempting to cover up the data breach. (United States Attorney's Office, 2022)

3.4 Consequences of the 2016 data breach

The personal consequences of the data breach for Joseph Sullivan are likely to be severe. Having been convicted by jury in 2022, he faces a maximum sentence of eight years’ imprisonment (Chesnut, 2022).

Uber has agreed to pay the following financial settlements in respect of the 2016 data breach:

- $148 million in the USA (Attorney General of Texas, 2018)
- £385,000 in the UK (Denham, 2018)
- €600,000 in the Netherlands (Autoriteit Persoonsgegevens, 2018)

Uber has not stated whether the attackers who infiltrated its GitHub repositories stole any of the company’s source code. However, from the publicised facts of the 2014 and 2016 data breaches, it would appear that the hackers had the opportunity to download source code. If a group of hackers obtains a company’s source code, it would present them with several possibilities:

- Sell the source code to one of Uber’s competitors
- Identify sensitive technical information such as encryption keys
- Use the source code to identify further vulnerabilities that could be used to hack into Uber’s systems again

3.5 Conclusions

The 2016 Uber data breach is a lesson in the importance of securing a company’s systems and intellectual assets (in this case, access to its GitHub repository and a database of customers and employees). The financial penalties for inadequate security may be high, and failure to properly respond to a security incident can have wider-ranging impacts, such as a loss of customer or employee confidence.

4 Legal protections

4.1 Registration of intellectual property

This section begins the examination of the theory of protecting intellectual assets.

One form of protection available to owners of intellectual assets is to register their assets. However, in doing so, the owner may relinquish the secrecy of the intellectual property, as explained below.

The forms of registration available in the EU are as follows:

1. Copyrights
2. Trademarks
3. Patents
4. Utility models
5. Design rights

Each category applies to different types of intellectual assets, and each offers different protections.

4.1.1 Copyrights

Copyrights are rights held by authors (copyrights or author's rights) and performers, producers and broadcaster (known as related rights) (Directorate-General for Communications Networks, Content and Technology, 2022). In the EU and in every country that is a signatory to the Berne Convention, copyrights are granted automatically. In other words, there is no need for copyrights to be explicitly registered, although some countries have national legislation enabling registration. Applying for registration may facilitate the enforcement of copyrights by establishing key information such as the date of authorship (European Commission, 2023).

Copyrights only apply to the specific form in which an idea is expressed, whether it be in writing, illustration or performance; they do not apply to the underlying idea. Copyrights can, therefore, apply to the source code of a computer program but not to its actual technical functionality. In other words, it would be a breach of copyright to copy, line-for-line, an author's computer code and exploit it for commercial gain. However, using the idea of the code to write one's own routines or program that achieve a similar outcome as the original code would not be a breach of copyright. (European Commission, 2023) For example, it would be a breach of copyright to copy the source code of Google Maps and use it to launch a new online mapping service. Conversely, building a new online mapping service from the ground up (without copying source code) is not a breach of copyright, even if the functionality of the new service is substantially similar to that offered by Google Maps.

The enforcement of copyrights is largely subject to national rather than EU-wide legislation, although the European Union has taken steps towards the harmonisation of copyrights in the context of the “information society” (Griffiths, 2013). Consequently, rights holders may incur high legal expenses for enforcing copyrights in different territories.

4.1.2 Trademarks

A trademark is a sign that uniquely identifies a company, product or service as distinct from any other company, product or service (World Intellectual Property Organization, 2023). For many businesses, the trademark is an essential part of its identity, and it may be the most valuable intellectual asset the company owns.

Trademark protection is available through registration, and a European Union trademark offers protection throughout the European Union. (European Union Intellectual Property Office, 2023) Under Article 9 of the European Union Trade Mark Regulation[1], registration confers “on the proprietor exclusive rights” to use the trademark and, hence, prevent other parties from using it. (Eur-Lex).

In effect, trademark legislation prevents a company from marketing itself or its products or services using the registered trademarks of another company. For example, it would be a trademark infringement for any company other than Apple Computer Inc. to market computer hardware under the name “Apple” or using an apple as a logo.

4.1.3 Patents

A patent is an exclusive right to exploit an invention, which is a novel way of doing something or a new solution to an existing problem. (World Intellectual Property Organization, 2023) Patents must be registered, and the registration must include a detailed description of the invention. The authorities use the description to determine whether the invention is eligible for a patent based on the following criteria:

- Novelty

  The invention must be new in relation to the “prior art”, i.e., the inventions and methods that were public knowledge at the time of registration.

[1] Regulation (EU) 2017/1001 of the European Parliament and of the Council on the European Union trade mark

- Inventive

  The solution must include an inventive aspect that was not public knowledge before registration and that is not an obvious step to a person skilled in the field.
- Industrial applicability

  According to the Finnish Patents and Registration Office, patents must be “technological in nature”, solve technical problems and have practical applications. In that sense, an idea or theory would not qualify for a patent, whereas an industrial process, method or device would.

  In this context “industrial” refers to broadly to all areas of commercial activity; not only traditionally industrial applications, such as manufacturing. (Finnish Patent and Registration Office, 2023)

Patents grant the rights holder an effective monopoly over the invention, preventing other entities from using it. As per Article 63 of the European Patent Convention, the lifetime of a European patent is 20 years, although Contracting States may choose to extend the period (European Patent Office, 2000). When the patent expires, the invention enters the public domain, and other parties may use it freely. The pharmaceutical industry provides a well-known example of this: a company develops a new drug and patents it. While the patent is valid, the company has a monopoly on the sale of that particular active substance. When the patent expires, competing generic versions of the same drug appear on the market, as other pharmaceutical companies are then entitled to manufacture the same product.

The monopoly provided by patent registration offers a clear advantage to businesses: an exclusive period in which they can exploit their invention and the associated first-mover advantage. This enables them to build up brand value, which they may continue to exploit after the expiry of the patent by charging more for their product than for technically identical products from different manufacturers.

However, there is also a clear downside. In order for the patent authorities to evaluate the uniqueness of an invention, the invention must be disclosed in detail. Patents are published, so when they expire, any party can access the details to discover exactly how to replicate the invention. A further disadvantage is the time taken to process applications: it can take three to five years from the date of application to obtain an EU patent (European Patent Office, 2023).

Questions surround the patentability of computer programs. Under Articles 52(2) and 52(3) of the European Patent Convention, computer programs may only be patented if they have a “technical character” that produces a “further technical effect” when run on a computer (European Patent Office, 2023).

4.1.4 Utility models

Like a patent, a utility model can cover a technical solution with an industrial application. It can also protect chemical compounds, foodstuffs, pharmaceutical products and microbiological inventions. However, utility models cannot cover methods or uses – a patent is required for these. Utility models are required to be inventive, although the standard of distinctiveness from the prior art is less stringent than for patents: utility models must have a “clear” distinction from existing techniques, whereas patents must have an “essential” difference. (Finnish Patent and Registration Office, 2019)

When a utility model is registered, it affords the holder the exclusive right of exploitation.

4.1.5 Design rights

Design rights apply to the appearance of a product, or part thereof, based on its “lines, contours, colours, texture and/or materials”. The design is required to be novel and individual. Design rights can be registered with the national authorities in individual countries or by applying for a Registered Community Design, which offers protection throughout Europe. Design protection is also afforded by Unregistered Community Designs, although the protection is weaker than for Registered Community Designs (Your Europe, 2022).

Design rights can protect a company’s brand value by preventing other parties from selling products that look substantially similar.

4.2 Trade secrets

Before we can conclude the analysis of the available forms of protection, we must identify the meaning and significance of trade secrets. Article 2(1) of the EU Trade Secrets Directive[2] defines a trade secret as:

“*information which meets all of the following requirements: | (a) | it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; | (b) | it has commercial value because it is secret; | (c) | it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;”* (European Parliament and Council, 2016)

[2] Directive (EU) 2016/943 of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

The above definition is derived from the protections on undisclosed information enshrined in Article 39(2) of the World Trade Organization’s TRIPS Agreement[3], which is applied in all WTO member countries. This agreement sets out an international framework for the protection of intellectual property. (World Trade Organization, 1994)

However, it is relevant to consider the definition in the European Directive because the same – or a substantially similar – definition is implemented into the national legislation of all states in the European Economic Area. (For example, the Trade Secrets Act (595/2018) in Finnish legislation (Finlex, 2018).) It is justified to consider the legal definition of a trade secret – rather than any other definition – because the legal system is the principal form of recourse in the event of the theft of a trade secret. It is unfeasible to expect intellectual property to be effectively recovered, and taken out of the possession of third parties, by any other means.

In sum, the above definition, therefore, requires a trade secret to be innovative, valuable and protected.

4.3 Legal recourse for intellectual property infringements

Several forms of protection and redress exist for registered intellectual assets.

The possible protective measures include legal recourse under intellectual property, competition and criminal legislation (Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs, 2013).

4.3.1 Damages

The means of restitution include retrospective relief in the form of damages, which serve both to indemnify the rights holder and deter potential or recurrent infringement (European Observatory on Counterfeiting and Piracy, 2010).

However, according to the European Observatory on Counterfeiting and Piracy, the assessment of damages faces a number of shortcomings. Chiefly among these shortcomings is the difficulty in assessing the amount to award in damages. Article 13 of the Property Rights Enforcement Directive (IPRED)[4] calls for courts to measure damages “appropriate to the actual prejudice”

[3] Agreement on Trade-Related Aspects of Intellectual Property Rights as Amended by the 2005 Protocol Amending the TRIPS Agreement

[4] Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights

suffered by the injured party whose intellectual property rights are infringed by another party either knowingly or “with reasonable grounds to know” (Eur-Lex, 2004). The Directive offers two avenues for such as assessment:

1. All negative economic consequences that the rights holder suffers, including lost profits and unfair profits made by the infringer. This provision also includes the potential for non-economic factors such as “moral prejudice” (reputational damage, among other things).
2. A lump sum based on factors such as the amount the infringer would have had to pay to use the intellectual property right with authorisation.

The European Observatory on Counterfeiting and Piracy notes that the courts of almost all European countries consider the amount of lost profit, defined as the amount the rights holder would have made in the absence of any infringement, when they assess damages. However, the Observatory points out that such lost profits are difficult to calculate accurately, so the courts of many countries opt for option 2 above, i.e., a lump sum award approximating the lost profits or moral damages (European Observatory on Counterfeiting and Piracy, 2010).

Furthermore, despite the intention of IPRED Article 13 to provide for damages covering the “actual prejudice”, many negative economic consequences and infringer profits are not taken into consideration. The European Observatory on Counterfeiting and Piracy notes that courts in Finland, among other countries, do not take into account many types of consequential damage, such as reputational damage, lower prices and loss of brand or trademark value.

IPRED Article 14 requires the unsuccessful party in a legal action to bear the “reasonable and proportionate” legal costs and expenses of the successful party (Eur-Lex, 2004). However, the European Observatory on Counterfeiting and Piracy as found that it can be difficult for plaintiffs to recover the full costs of legal action for intellectual property enforcement, as courts in some countries award legal expenses lower than those actually incurred (European Observatory on Counterfeiting and Piracy, 2010). Consequently, even when a court fully indemnifies the rights holder for the infringement (in other words, if the court awards the full amount in damages under the law), if the court does not award the full amount of legal expenses, the plaintiff’s outcome from the enforcement proceedings will be a net negative.

On top of this, infringers may also be able to retain some of the profits of their activities. The Observatory concludes that if the maximum disadvantage suffered by an infringer is less than or equal to the normal licence fee, the system serves to incentivise infringement, not deter it (European Observatory on Counterfeiting and Piracy, 2010).

4.3.2 Provisional or precautionary measures

Given that the legislation on damages has a weak deterrent effect (or even the opposite of such an effect) and may also deter civil enforcement actions, what other aspects of legislation may help to protect against intellectual property rights infringement?

IPRED Article 9 sets out a framework for provisional and precautionary measures (injunctions) to forbid imminent infringement or stop ongoing infringement. It also provides for the seizure of the infringer's property and freezing of assets, such as bank accounts, in the event of infringement on a commercial scale. (Eur-Lex, 2004)

IPRED Article 11 provides for injunctions and penalties for failure to comply with injunctions. (Eur-Lex, 2004)

A separate report by the European Observatory on Counterfeiting and Piracy concerning injunctions notes that precautionary measures may be imposed without hearing the defendant due to the inherent urgency of such cases. This mainly occurs when the rights holder is unlikely to recover damages or evidence may be destroyed. In these cases, the rights holder must prove that they own the right and may sometimes be required to pay a security deposit, which could be used to compensate the defendant if the case is decided against the rights holder. (European Observatory on Counterfeiting and Piracy, 2009)

The European Observatory on Counterfeiting and Piracy noted that the injunction rights provided by IPRED Articles 9 and 11 are available and widely used in Member States, in some cases even as the primary means of enforcement. The Observatory notes that courts are willing to impose precautionary measures and impose them quickly. This has the effect of forcing the defendant to the negotiating table: if they wish to continue using the intellectual property rights they have infringed, they must negotiate a licence. (European Observatory on Counterfeiting and Piracy, 2009)

However, the Observatory also notes that the framework of provisional and precautionary measures suffers from the disadvantage of high up-front costs for the rights holder, including the security deposit, legal expenses and any applicable bailiff's fees.

In cases involving intermediaries such as internet service providers and web hosts, data protection legislation may effectively prevent the disclosure or discovery of information necessary during the evidence-gathering stage. In other words, if it is not possible to identify who the defendant is, the rights holder cannot bring legal action.

Furthermore, the Observatory finds some of the sanctions to be too small to be effective deterrents, so the infringement does not stop. Consequently, the rights holder's only hope of a remedy may be a subsequent award of damages. This suffers from the problems described in section 4.3.1.

4.3.3 Legal protections for trade secrets

Trade secrets are also protected by legal provisions providing for injunctions, precautionary measures, indemnity and damages, and compensation for use in a manner similar to that described in sections 4.3.1 and 4.3.2 above.

In addition, violations of trade secrets may be subject to penalties under chapter 30, section 4 of the Criminal Code of Finland covering "business espionage", in addition to the penalties provided in chapter 30, section 5 of the Criminal Code on violations of business secrets. Accordingly, the punishments for violations are a fine or up to two years' imprisonment. (Finlex, 2022)

In Finland, the Employment Contracts Act prohibits employees from unlawfully utilising the employer's trade secrets and disclosing them to third parties. The Act also attributes liability for damages to both the employee divulging a trade secret and the recipient of the information, if the recipient "knew or should have known" that the trade secret was obtained unlawfully (Finlex, 2019).

4.4 Contractual clauses

The employment contract offers other avenues for companies to protect their trade secrets. Employers can include confidentiality clauses in employment contracts. Finnish law allows for confidentiality obligations to survive the end of an employment relationship for up to two years (Criminal Code, chapter 30, section 5(3) (Finlex, 2022)). However, when two years have elapsed from the end of an employment relationship, a former employee can no longer be punished for divulging business secrets.

Other contractual avenues for protection include restrictive covenants. These may include the following:

- A **non-compete clause** restricts former employees from working in similar roles for competitors
- A **non-solicitation clause** prevents former employees from taking action to steal customers or suppliers away from the former employer
- A **non-dealing clause** restricts former employees from engaging in any deals with the former employer's customers or suppliers, even if the said parties approach the former employee

- A **non-poaching clause** prevents former employees from enticing their former colleagues to leave the organisation (Pinsent Masons, 2023)

In Finland, non-compete clauses may only be imposed for a “particularly weighty reason” for a maximum term of six months. If compensation is paid to the employee, the term can be extended to one year. It should be noted that according to the law, “keeping a trade secret” may qualify as a sufficiently weighty reason for a non-compete clause, depending on the nature of the employer’s activities. Furthermore, the non-compete clause does not apply if the employer terminates the employment (Employment Contracts Act (Finlex, 2019)).

The aim of a non-compete clause is to prevent the employee from taking the employer’s business secrets to a competitor. By mandating a certain length of time away from the business sector, the employee’s knowledge can be assumed to become less relevant and valuable, although that is by no means inevitable.

It should be noted that the US Federal Trade Commission has proposed banning non-compete clauses on the grounds of their detrimental impact on competition and the labour market (Federal Trade Commission, 2023), so developments in this area may be a concern for organisations relying on trade secrets as a means of protecting their intellectual assets.

5 Physical and structural security

The company’s premises, such as office and production buildings, should be secured to prevent third-party intrusion. ISO 27002:2013 stresses the importance of a physical barrier to protect an organisation’s property. (International Organization for Standardization, 2013)

This section discusses some of the forms of physical protection.

5.1 Building standards

Depending on the location, the enterprise may need to consider selecting a building with sufficient structural strength, safety in use and fire protection.

In Finland, the Land Use and Building Act and the National Building Code of Finland, a collection of regulations and instructions supplementing the Land Use and Building Act, mandate strict standards for new buildings zoned as business premises. These include specifying minimum standards of structural endurance in the event of a fire and requiring the design to enable the evacuation of people inside it in the event of a fire (Finlex, 1999; Ministry of the Environment, 2023).

5.2 Access control systems

Unauthorised parties should be prevented from easily accessing the enterprise’s buildings. Depending on the scale of the organisation, the following measures may be applicable:

- Lock and key
- Electronic access control system
- Manned reception desk

These measures offer a minimum standard to ensure that a person could not simply walk into the working premises from the street and gain access to the enterprise’s premises and information.

Access card systems and reception desks may also provide physical log books and electronic audit trails of entries to and exits from the building, facilitating the work of forensics in the event of a criminal offence. (International Organization for Standardization, 2013) For example, ASSA ABLOY, which claims to be the market leader in access control solutions (ASSA ABLOY, 2021), currently offers nine access control systems, with ancillary cloud-based services providing information about access transactions.

Figure 1 illustrates the operating principle of an electronic access control system, where the host PC or main control panel is responsible for determining whether the user is entitled to access the area and logging all access requests.

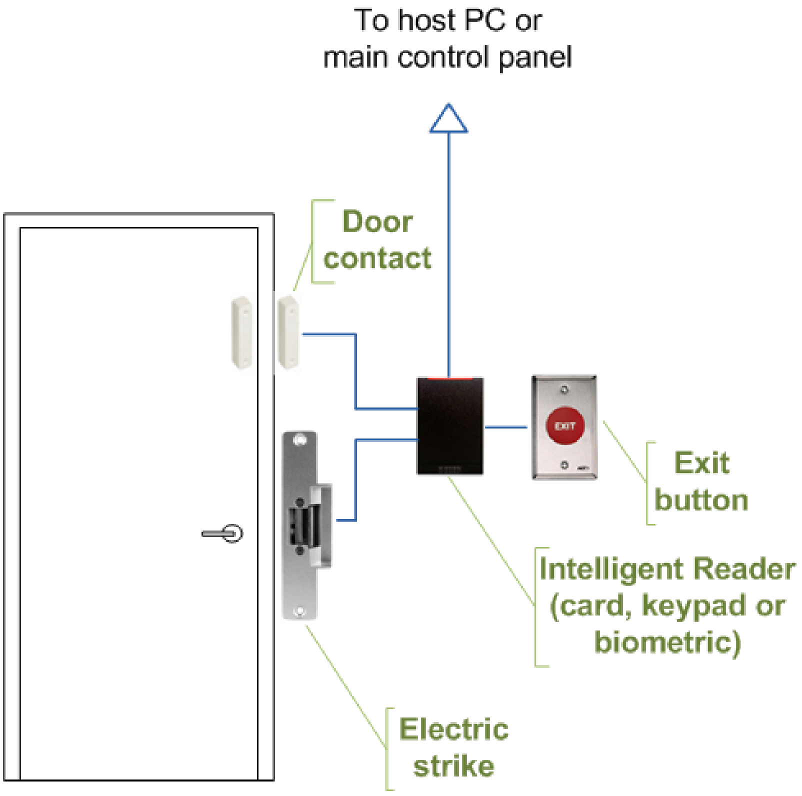


Figure 1. Operating principle of an electronic access control system. Source: Wikimedia Commons

5.3 Intruder detection systems

The external doors and windows of the enterprise's premises should be equipped with an intruder detection system. Buildings should also be checked to ensure there are no weak spots from which an intruder could readily gain access to the building. (International Organization for Standardization, 2013)

5.4 Location of valuable assets within a building

The enterprise's most valued assets should be in a protected area inside the building. Care should be taken to ensure that such asset can only be accessed by the personnel who genuinely need them.

In addition, the potential for natural hazards should be considered. For example, if the area is prone to flooding, valuable assets should not be kept on the floor at ground level.

It may also be wise to allow for additional fire protection for valuable assets. For example, the National Building Code of Finland mandates certain standards of fire protection with a focus on evacuating people safely from the building. (Ministry of the Environment, 2023) The need to evacuate or protect property is not the primary consideration of such building standards. Consequently, an enterprise storing valuable information on paper could consider investing in a fireproof safe.

6 Organisational measures

This section examines some of the organisational measures a small or medium-sized enterprise should consider to ensure the protection of intellectual assets.

6.1 Training

Research by the World Economic Forum has found human error to be the root cause of 95% of cybersecurity risks (World Economic Forum, 2022). Potential topics for security training could include:

- Strong password standards
- Identifying phishing attacks and other forms of social engineering
- Understanding how data can be gathered
- Best practices for dealing with unsolicited email, especially messages with attachments and links
- Protecting hardware and software outside the office, including:
- Not leaving computers, phones or other mobile devices unattended in public places
- Making sure that other people cannot see what is displayed on the screen of a computer, phone or other mobile device
- Using only encrypted internet connections

6.2 Security policies

This section describes some security policies for organisations.

6.2.1 Classifying information according to sensitivity

ISO 27002 recognises four levels of information classification based on the potential impacts on an organisation’s operations if the information were revealed publicly.

The four confidentiality levels could be labelled as follows:

- Public

  Disclosure of public information would not harm the organisation. Furthermore, public information is intended for disclosure and the act of disclosure may benefit the organisation. Examples of public information include press releases.
- Internal

  Internal information is available to all personnel within the organisation. Internal information is not intended for public disclosure, although the disclosure of information in this classification would be unlikely to severely damage the organisation. In the wording of ISO 27002, disclosure would cause “minor embarrassment or minor operational inconvenience” (International Organization for Standardization, 2013). Examples of internal information include standard operating procedures for activities that are not business-critical, such as purchasing lunch from a staff canteen.

- Confidential

  Confidential information is intended to be kept secret. Personnel may be granted access to confidential information if they need it for their jobs and they should not disclose it to anyone else. If confidential information is disclosed, it could lead to severe short-term harm to the organisation and prevent it from achieving its tactical goals. Examples of confidential information could include details on pricing in customer contracts: if such information became public, the organisation’s competitors would gain valuable information that may help them to win contracts from the disclosing organisation.

- Restricted/secret

  Restricted information is the most secret form of information. Disclosure of restricted information could cause significant harm to the organisation’s reputation and business potential or expose it to legal ramifications. Examples of restricted information include sensitive customer data, especially in areas such as health care, where information must be kept secret.

6.2.2 Removal rights

According to ISO 27002, “equipment, information and software should not be taken off-site without prior authorization”. (International Organization for Standardization, 2013) This is a straightforward rule that should be easy for personnel to understand: an employee should always ask for permission before taking any of the organisation’s information off the premises.

At least two factors complicate this, however.

Since the advent of hybrid work on a large scale (see section 2.2), the boundaries between the workplace and off-site have become blurred. If an employee has an agreement with the employer on remote working, the employee will, by definition, need to take the organisation’s equipment, information and software off the site. The employee may have a reasonable expectation that all the equipment, information and software they normally use in the office can also be taken off-site; otherwise, the employee’s productivity may be impacted. This problem can be mitigated by drafting specific work-from-home policies regarding the information that can be taken off-site.

Secondly, hybrid work has introduced new security vulnerabilities. For example, during the initial lockdown (stay-at-home) period of the coronavirus pandemic, the number of daily meeting participants using videoconferencing platform Zoom rocketed from 10 million to more than 200 million by March 2020. (Yuan, 2020) In tandem with this development, the practice of Zoom-bombing became more prevalent. Zoom-bombing involves an infiltrator joining a Zoom meeting uninvited, potentially gaining knowledge of sensitive information. (University of Oxford, 2020) This issue can be mitigated by setting up Zoom meetings securely, using passwords and specific invitations, rather than making them publicly available.

6.2.3 Regular reviews of access rights

Throughout employment, organisations should regularly check whether their employees have appropriate access rights and revoke any unnecessary rights. For example, if an employee working on a specific product moves to a different role within the organisation, the employee’s access to the product should be revoked.

6.2.4 Offboarding policy

In line with ISO 27001, organisations should have a sound procedure in place for the end of employment. When an employee’s employment ends for any reason, the employee must be required to return all company assets, whether information, hardware or software. (International Organization for Standardization, 2022) Here, it should be noted that employees may have made copies of the organisation’s information for legitimate work-related reasons, such as needing to take information off the premises in order to work from home. Organisations should take care to ensure that employees do not retain any such information. This could be achieved by asking the employee to sign an affirmation including a financial penalty for non-compliance.

The employee should also be reminded of any post-employment clauses in the employment contract that are intended to survive the cessation of the contract, such as non-compete clauses (see section 4.4 for a more exhaustive list).

A study conducted by Osterman Research in 2014 found extensive shortcomings in the post-employment policies of small and medium-sized businesses, with 89 per cent of former employees retaining access to sensitive corporate applications, such as SharePoint and Salesforce, and 49 per cent logging in after leaving the company. (Osterman Research, 2014)

6.3 Security in a hybrid work setting

Hybrid working is gaining traction throughout the knowledge economy (see section 2.2). For some organisations, this presents the potential for new security risks. As hybrid working has become so prevalent, the inherent security risks are covered as aspects of the relevant sections of this report, rather than as distinct entities.

7 Software security

7.1 Authentication

7.1.1 Password standards

Numerous standards refer to password complexity and security. Table 2 compares the requirements of various standards in this field.

Table 2. Password complexity factors recommended by security standards. Sources: OWASP (OWASP, 2023), OWASP ASVS (OWASP, 2021), NIST (Grassi, et al., 2020) and PCI-DSS (PCI Security Standards Council, LLC, 2022)

Requirement	OWASP	OWASP ASVS	NIST	PCI-DSS
Minimum password length (L, characters)	$L \geq 8$	$L \geq 12$	$L \geq 8$	$L \geq 12$
Maximum password length (L_{max}, characters)	$L_{max} \approx 64$	$64 < L_{max} < 128$	$L_{max} \geq 64$	
Do not truncate the password	✓	✓	✓	
Permit all ASCII characters	✓	✓	✓	
Permit Unicode characters	✓	✓		
Require a certain mixture of alphanumeric and special characters			×	✓
Compare passwords against a password dictionary		✓	✓	(history)
Permit “paste” functionality		✓	✓	
Require a new password to be set in the event of a password leak	✓	✓	✓	
Enforce password rotation		×	×	✓
Limit the number of failed login attempts (F)			✓	$F \leq 10$

In Table 2, a tick mark (✓) indicates that the standard explicitly recommends the stated action. A cross mark (×) indicates that the standard explicitly forbids the stated action. An empty cell indicates that the standard does not advise on the action either way.

In this table, “truncation” refers to shortening passwords before they are hashed or stored. Three of the standards explicitly forbid truncation. PCI-NSS advises requiring users to have a mixture of letters and numbers in their passwords, while NIST explicitly advises against this. OWASP ASVS, NIST and PCI-DSS advise checking passwords against a dictionary of some type: in the case of PCI-DSS, the user is not allowed to reuse their old passwords, whereas the other standards advocate comparing passwords against a corpus of breached passwords, dictionary words and easy-to-guess passwords. Two of the standards require the “paste” functionality to be permitted. This is essential for using a password manager, which automatically inserts the correct password into the password field when logging in.

ISO 27002 does not set any specific standards for secure passwords in terms of the length and range of characters required. Instead, it recommends enforcing “quality passwords” (International Organization for Standardization, 2013).

Password rotation appears to be a particularly thorny issue: ISO 27002 and PCI-DSS both recommend enforcing periodic password rotation. Conversely, OWASP ASVS and NIST explicitly advise against arbitrary password rotation policies. OWASP, OWASP ASVS and NIST recommend that users be required to change their passwords following evidence of a password leak.

7.1.2 Password management

A survey by Nordpass found that 7/10 people in the UK and US had over ten password-protected accounts and 2/10 had more than 50. They survey also found that people have difficulty remembering their passwords. (Rawlings, 2020) Password managers, such as LastPass, can generate separate random secure passwords for each site or app and store them so that users do not need to remember them. The password manager is protected by a single master password and can also be protected by multifactor authentication (see section 7.1.3).

7.1.3 Multifactor authentication

Multifactor authentication is defined by the US Department of Commerce as:

> Authentication using two or more factors to achieve authentication. Factors are (i) something you know (e.g., password/personal identification number); (ii) something you have (e.g., cryptographic identification device, token); and (iii) something you are (e.g., biometric). (Newhouse, et al., 2019)

Although not specifically mentioned here, a mobile phone can also qualify as “(ii) something you have”. Given the ubiquity of mobile phones, the easy approach to multifactor authentication is to require verification from a mobile phone in addition to a password. This can be achieved using a third-party authenticator app, such as Microsoft Authenticator, with compatible software.

For web apps, a new option that enjoys the backing of the most popular browsers and mobile operating systems is Passkeys. This is an implementation of the WebAuthn component of the FIDO2 specifications from the FIDO Alliance, and it provides an API for web app developers to require a second factor during authentication. Upon logging in, the user is asked to use one of their other devices, such as a mobile phone or cryptographic device, to confirm the login. (FIDO Alliance, 2023)

7.2 Standardised software

Organisations should standardise the software their employees use, so that they only use pre-approved software. Besides helping to avoid the potential for rogue apps to steal data from the user (and, by extension, the organisation), it could also help to reduce the organisation’s support costs.

As regards desktop apps installed locally on the computer, Windows Defender Application Control can limit the range of apps that users can install based on policies. It can be used in combination with AppLocker to restrict the apps that are allowed to run on a computer. (Microsoft, 2022) As a centralised solution, Microsoft offers Intune, which integrates identity, application and device management, including mobile devices. Intune is compatible with Android, iOS, iPadOS, macOS and Windows client devices. (Microsoft, 2023) Apple offers the Apple Business Manager, part of its platform deployment system, to achieve a similar end result, although it is limited to Apple’s macOS, iOS and iPadOS devices. (Apple, 2022)

These device management solutions ensure that employees only use the approved applications on their devices and allow the organisation to update software when necessary, including updating the operating system. (Microsoft, 2023)

A potential difficulty in deploying device management solutions is the prevalence of Bring Your Own Device (BYOD) policies in organisations. A study by Cybersecurity Insiders found that 82 per cent of organisations enable BYOD to some extent, with almost half of the surveyed organisations experiencing a significant increase in the number of people using BYOD due to the shift to remote work (Cybersecurity Insiders, 2021). It should also be noted that BYOD may apply to a wider group of individuals than just the employees of an organisation: Cybersecurity Insiders noted that 61 per cent of the “extended workforce”, consisting of contractors, partners and suppliers, used BYOD.

The obvious risk of BYOD is that personal devices could contain rogue apps or malware, which could expose or steal the organisation’s information. A Mobile Device Management (MDM) policy can help in this regard. BYOD users are asked to enrol in the MDM service, which can mandate the installation and use of anti-malware software. Enrolled devices can then be configured for better security. (Microsoft, 2023)

A further potential difficulty with BYOD concerns the action to take if the device is lost. Microsoft Intune allows lost devices to be located, potentially aiding in the recovery of the device. A managed device owned by the organisation can be remotely locked or wiped if it is lost or stolen. (Microsoft, 2023) However, remotely wiping a user’s personal device is somewhat more fraught: the user’s personal data may also be lost in the wipe.

Possible alternatives to the local installation of applications and storage or data are to use cloud-native applications or Desktop as a Service (DaaS) solutions, which are discussed in section 9.4. The advantages of these solutions are that they are device-agnostic, so users can access them with a very wide range of devices, including tablet computers and mobile phones, as well as conventional computer workstations. They are also independent of the user’s local operating system, so they would work effectively with a BYOD policy.

7.3 Anti-malware software

Microsoft provides Windows Defender with the Home, Pro and Server editions of Windows. This software is an endpoint protection solution that scans files to detect malicious signatures against a database of known threats. If it detects malware, it can quarantine the infected files and, in some cases, disinfect them. Apple touts the security of its custom hardware and other subcomponents, including the T2 Chip and Secure Enclave.

7.4 Encryption

7.4.1 Storage devices

Data should be encrypted so that if the hardware falls into the wrong hands, a malicious actor will be unable to exploit the data. All editions of Windows 11 except the home edition come with BitLocker, which encrypts the computer’s hard drives. Other encryption software is also available for this purpose.

7.4.2 Communications

Today, HTTPS has become the standard for worldwide web communications. This ensures that traffic between a client and server is encrypted using transport layer security (TLS). TLS effectively guards against man-in-the-middle attacks, whereby a malicious actor could intercept communications between a client and server to gain valuable information or tamper with the information en route to its destination. Encryption renders the information inherently worthless without the cipher key required to decrypt it. The organisation’s web services should use HTTPS by default.

Today, most other forms of communication are encrypted by default: Slack encrypts messages at rest and in transit (Slack, 2023), and end-to-end encryption can be activated for Teams calls on individual machines, by using policies or via the Teams admin centre (Microsoft, 2022).

7.4.3 Hashing

Certain types of sensitive data can undergo one-way encryption, also known as hashing, to ensure security. For example, passwords should be passed through a hashing algorithm before being stored in a database. The algorithm outputs a fixed-length ciphered string. The following factors affect the resulting hash:

- Hashing algorithm
    - OWASP currently recommends Argon2id, which won the 2015 Password Hashing Competition (OWASP, 2023)
- Number of iterations
- Salt
    - A string combined with the password to make the input more complex
    - When separate salts are applied to each password, the hash output by the hashing algorithm will be different, even when two users have the same password

Hashing ensures that in the event of the loss or theft of the password database or table, an attacker will be unable to determine users’ passwords because they are not stored in plain text. The only way to discover passwords based on hashes is to repeat the hashing process. Even if the attacker knows the hashing algorithm, number of iterations and salt for each password, the process of trying a long list of potential passwords is computationally very costly and, therefore, time-consuming. Ideally, an attacker should be unable to determine the algorithm, number of iterations and salt, thereby further complicating the process of cracking hashed passwords.

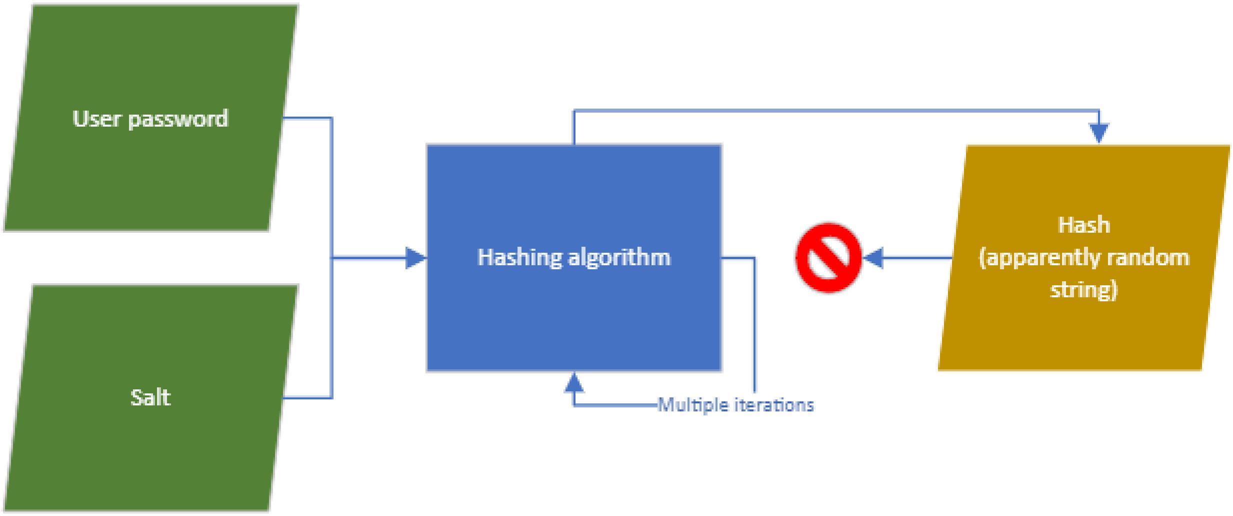


Figure 2. Principle of one-way encryption (hashing)

7.5 Development according to security frameworks

For organisations that produce software, the OWASP Foundation provides public, open-source information to enhance the security of software. One essential measure in software development is to analyse the organisation’s software in accordance with the OWASP Top Ten, which, according to OWASP, “represents a broad consensus about the most critical security risks to web applications”. (OWASP, 2023)

As the range of software developed by organisation can vary dramatically, it is not the goal of this report to provide an exhaustive list of software security sources. However, it is essential for software developers to be aware of the security implications of their products.

8 Hardware security

8.1 Privacy filters

Privacy filters are layers of material placed over a screen to reduce the viewing angle. They use optical techniques to filter out light from the screen to all angles except a reasonable subset in the field of vision of a user directly in front of the screen. This prevents eavesdropping and “visual hacking”. (3M, 2023)

8.2 Device locks

Kensington locks can be used to physically secure devices to a table, anchoring point or other hard-to-move object. This prevents devices from being stolen easily. Kensington lock slots are present on many modern laptops, and the locks themselves are available in a range of sizes to suit all computer form factors. (Kensington, 2023) Locks can require a physical key or number combination to open them.

8.3 Biometric security

Computers can be configured to require a fingerprint to unlock them. Many enterprise laptops have integrated fingerprint readers. For example, at the time of writing, Lenovo offered 284 products with integrated fingerprint readers. (Lenovo, 2023)

For devices without integrated biometric hardware, a separate USB fingerprint reader can be added at little additional expense. (Kensington, 2023) This may be a suitable solution for organisations operating with a BYOD policy.

Apple’s mobile devices currently enable Face ID, a method for unlocking the device using facial recognition. A similar feature is provided by Windows Hello. Apple quotes the probability of a false positive unlocking via Face ID at 1 in 1,000,000 (0.0001%) (Apple Computer, 2022), while Microsoft quotes a false acceptance rate of <0.001% for facial recognition on Windows Hello (Microsoft, 2023). Kensington quotes a false acceptance rate of 0.002% for its cheapest USB fingerprint reader, decreasing to 0.001% for more expensive products (Kensington, 2023).

Windows Hello also offers iris recognition, although it requires an expensive HoloLens 2 device and has a false acceptance rate of 1 in 100,000 (0.001%) (Microsoft, 2023). Consequently, iris recognition would not appear to offer superior security in comparison with a significantly cheaper fingerprint reader.

All of the biometric solutions discussed above are suitable for use as an additional factor in multifactor authentication (see section 7.1.3).

8.4 Hardware encryption

Many modern devices integrate encryption at the hardware level. Apple computers with the T2 Chip automatically encrypt data, so encryption does not need to be specifically switched on.

In addition, self-encrypting drives (SEDs) are available for data storage. These devices encrypt the data as it is written to the medium using a factory-set disk encryption key (DEK). In auto-lock mode, an SED uses an additional authentication encryption key (AEK), which is required to unlock the device after it has been powered down. A valid AEK is required to read the DEK in order to execute read and write operations. Without the DEK, the contents of the medium remain encrypted and, consequently, cannot be accessed. Since SEDs with this setting enabled are automatically locked when they power down, there would be no benefit for an attacker in stealing the physical storage medium unless the hacker could also steal the AEK. (IBM, 2022)

8.5 End of lifecycle of storage media

ISO 27002 recommends either physically destroying devices containing sensitive data or securely erasing the data. (International Organization for Standardization, 2013)

Many enterprise-grade storage devices are self-encrypting drives (SEDs), which have always-on encryption. The user cannot turn the encryption off, so it is unlikely for any unencrypted data to remain on an SED. The data on an encrypted device, such as an SED, can be rendered inaccessible by a technique known as cryptographic erase (CE). CE sanitises the encryption key, leaving behind only inaccessible encrypted data. Since the encryption key is removed, it will be impossible to recover the data. The National Institute of Standards and Technology of the US Department of Commerce recommends using CE, provided that the drive always had encryption enabled. (Kissel, Regenscheid, Scholl, & Stine, 2014)

If the drive had unencrypted data stored on it before encryption was enabled, it may, potentially, be possible to recover the unencrypted data after CE sanitisation. In such a case, a more secure deletion strategy is to overwrite the sensitive data. Software or hardware products can identify the individual bytes on the drive and replace them all with zeros, ones or random data. However, there are also some limitations: storage devices using flash memory may have spare cells or use wear-levelling techniques to preserve data, which is then stored in areas that are not addressable using the standard read and write interfaces of the device. Some devices with built-in storage, such as mobile phones, may not even offer a way of overwriting data. Simply performing a factory reset on the device may not be enough to remove all traces of old data. However, if the device provides standardised data purging commands, it may be possible to bypass the abstraction layer of typical read/write commands and sanitise the entire medium. (Kissel, Regenscheid, Scholl, & Stine, 2014)

As a last resort, the device can be physically destroyed so that the entire storage medium is destroyed and not just damaged. This could be achieved by melting it, grinding it to dust or incinerating it. This may be the only option if the methods mentioned above cannot be used – for example, if the media has failed and does not respond to read, write or purge commands. (Kissel, Regenscheid, Scholl, & Stine, 2014)

9 Network security

9.1 Firewalls

Firewalls are positioned at the interface between a trusted network (the network belonging to the company or organisation) and an untrusted network (for example, the internet). Traditionally, the job of the firewall is to control inbound and outbound network traffic according to certain rules. Figure 3 illustrates how a firewall presents a barrier to internet traffic.

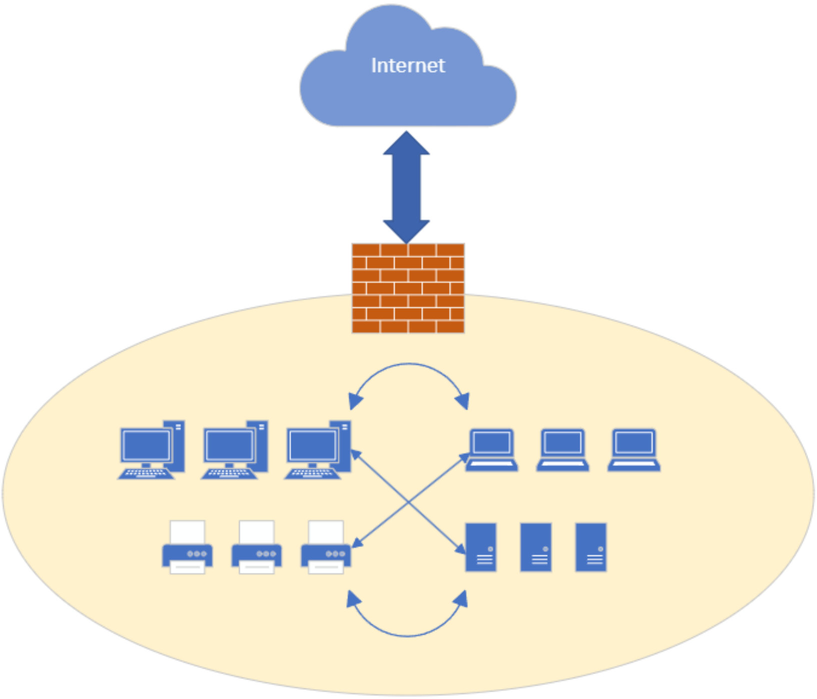


Figure 3. Principle of perimeter defence offered by a network firewall.

9.1.1 Stateful inspection firewalls

Traditional firewalls, known as stateful inspection firewalls, look at the state, port and protocol of traffic and determine whether to allow it or block it. They monitor the entire session of a connection, from the establishment to the closure of the connection, and dynamically decide whether to permit traffic. The decision is based on rules defined by the administrator and contextual information from previous connections and packets exchanged in the same connection. The firewall may also block or allow specific network ports and protocols. (Cisco, 2023)

An advisable strategy for working with stateful inspection firewalls is to start by blocking all inbound traffic. The organisation can then whitelist the specific protocols and ports that it needs.

9.1.2 Unified Threat Management (UTM) firewalls

UTM firewalls combine the functions of stateful inspection firewalls with additional features to combat threats such as intrusion, malware, spyware and leaks. They may also offer other network services, such as network address translation (NAT). (Kaspersky, 2023)

One advantage of combining several such services is that modernday threats are complex: they may combine different forms of malware and attacks on different parts of a network. In addition, a UTM applicance offers a single point of defence against external network threats. This allows network security services to be managed in one place, potentially facilitating configuration work. (Kaspersky, 2023)

However, it is also important to recognise that a single point of defence also means, by definition, a single point of failure: if the UTM appliance is compromised, the security of the entire network could be at risk. Consequently, it is wise for organisations to have a second layer of protection, such as software firewalls (see 9.1.4). (Kaspersky, 2023)

9.1.3 Next-generation firewalls (NGFW)

NGFWs expand on the protection afforded by a conventional stateful firewall by providing intrusion prevention, application awareness, threat intelligence, upgrade possibilities and techniques for meeting the challenges of new threats. (Cisco, 2023)

NGFWs can allow the microsegmentation of a network based on applications, not just ports, protocols and IP addresses. (Kaspersky, 2023) This could be valuable in a cloud context, where virtual machines may be started dynamically and, consequently, have only temporary IP addresses. In such a case, it is important to be able to restrict traffic according to the nature of the traffic itself rather than attributes such as the IP address.

A further advantage of a NGFW is its monitoring capability. This provides an organisation with a view of the activities underway in the network, including active applications, file transfers and websites. It helps the administrator to track the activity of threats across multiple users, devices and networks. (Cisco, 2023)

9.1.4 Software firewalls and other software-based network protection

The home, professional and server editions of Microsoft Windows all come with Windows Defender Firewall with Advanced Security, which is activated by default in home editions and can be activated for domains using the Group Policy Management Console on Windows Server. Microsoft recommends keeping the default settings, which block inbound connections by default and allow outbound connections. Organisations may choose more advanced configurations based on their workloads. For example, an administrator may choose to allow a certain app through the firewall, open a port or protocol, or permit certain types of traffic. (Microsoft, 2023)

Windows Defender also protects against other threats, such as malware and phishing (see section 7.3).

9.2 Microsegmentation

Microsegmentation is the concept of splitting a network into many smaller parts depending on the workloads. Each segment can then have granular security controls according to its requirements. Microsegmentation can also be applied to virtual machines so that individual applications can have specific security controls. The microsegmentation rules will determine whether two endpoints should access each other. (Palo Alto Networks, 2023)

For example, it may be appropriate for a web server to access a database server storing essential information for an organisation's web app. In contrast, there is probably no need for a database server to access the organisation's email server, so those endpoints could be in different segments and traffic between them could be blocked. This would preclude the possibility of a malicious actor accessing the organisation's email server via a compromised database server.

Microsegmentation, illustrated in Figure 4, inherently operates within a network, in contrast to a firewall (see section 9.1), which protects the perimeter of the network.

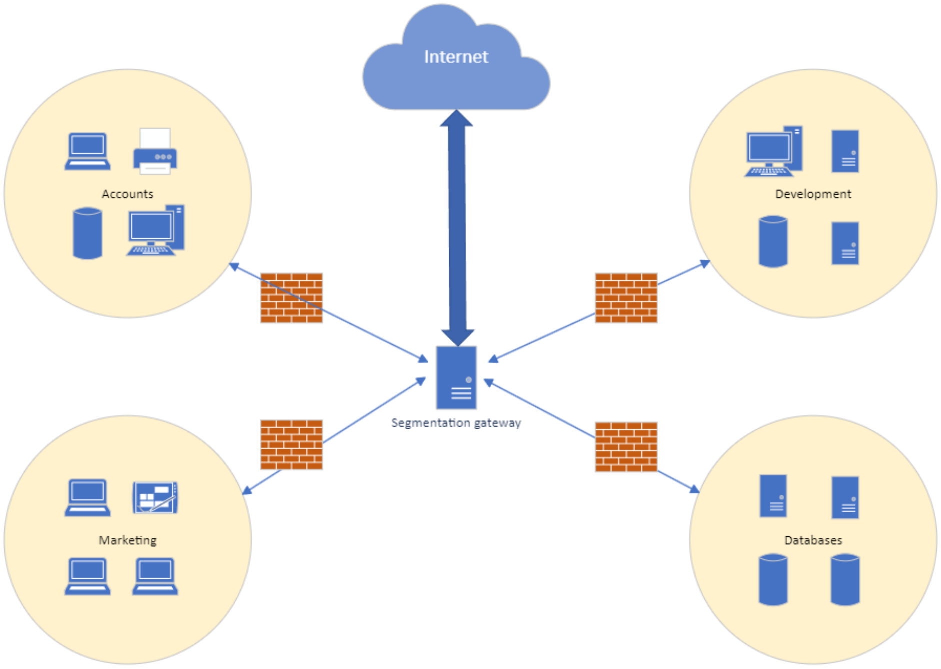


Figure 4. Example of microsegmentation according to business functions.

9.3 The Zero Trust Model

The Zero Trust Model, first proposed by John Kindervag in 2010, focuses on security inside a network. Kindervag says that “in Zero Trust, all network traffic is untrusted” (Kindervag, Build Security Into Your Network’s DNA: The Zero Trust Network Architecture, 2010) and proposes a complete rethink of network design.

Rather than defending the network perimeter (the attack surface) using a firewall and then applying separate controls inside the network, Kindervag advocates the use of “segmentation gateways”, which integrate all network security technologies and enable microsegmentation based on users, applications or data. Segmentation gateways determine which traffic is allowed to cross the micro-perimeters and access segments in a Zero Trust network.

Within segments, Zero Trust networks define “protect surfaces” – the smallest possible reduction of an attack surface. Protect surfaces are based on at least one of the following:

- Data
- Applications
- Assets
- Services

Kindervag says that the advantage of thinking about individual protect surfaces in this way is that they are “knowable”. This makes the task of defending a single protect surface more feasible than configuring a firewall at the ultimate perimeter of a company’s network. (Kindervag, Define a Protect Surface to Massively Reduce Your Attack Surface, 2018)

Above all, Kindervag stresses the strategic nature of the concept of Zero Trust: organisations should design their entire networks around Zero Trust, instead of using the technologies recommended in Zero Trust to address individual concerns. (Kindervag, You Want Network Segmentation, But You Need Zero Trust, 2019)

In practice, Kindervag uses physical or virtual NGFWs to serve as segmentation gateways in Zero Trust networks. (Kindervag, You Want Network Segmentation, But You Need Zero Trust, 2019)

9.4 Network security in a hybrid environment

Traditionally, employees have used virtual private networks (VPNs) to remotely access work networks. The VPN has acted as the “key to the door”, allowing the employee to cross the perimeter into the network and access the endpoints within. In a network protected solely by a firewall, the employee would then have access to the full range of attached endpoints. This represents a clear security risk in the event that the employee’s device is compromised, lost or stolen – a malicious actor could use the VPN to gain unfettered access to the organisation’s assets.

Companies specialising in networking are now promoting VPN-less hybrid work solutions implementing the Zero Trust model. For example, Cisco sells a remote access proxy that establishes a connection between a client and a specific application, rather than the entire network. (Kathuria, 2022)

According to a survey by HP, another alternative to VPNs is the Desktop as a Service (DaaS), with between 55 and 60 per cent of survey respondents in the finance, government & military, healthcare, media & entertainment, and technology sectors opting for DaaS technology to keep applications and confidential data within closer control of the organisation (HP, 2023).

10 Cloud security

Service providers provide a compelling case for cloud migration: AWS lists cost savings, higher productivity and fewer security incidents among the advantages. (Pastore, Fuller, & Gillespie, 2022)

Cloud service providers allow customers to replicate physical networks in virtual form, so virtual versions of all the network security solutions referred to in section 9 are available for cloud deployments.

AWS produces a checklist of security measures for cloud buyers (AWS, 2017), IBM has a guide on cloud security (IBM, 2023), Microsoft has several best practice guides on various aspects of cloud security, and Google has a whitepaper on security foundations on its cloud platform (Google, 2022). This section seeks to summarise some common best practices from these authorities:

10.1 Identity and access management (IAM)

IAM is the service that defines, enforces and manages user access policies for an organisation’s cloud services. Each user should have an individual account, and the IAM service determines which permissions are granted to each user. Access rights should be granted on the principle of least privilege – in other words, users should only be entitled to access the resources they really need to use.

IAM also makes it possible to enforce multifactor authentication and federate user identities with the organisation’s existing directory services, such as Active Directory. (Google, 2022) This facilitates the processes of adding new employees and, importantly, removing user accounts at the end of employment (offboarding, see section 6.2.4).

10.2 Data loss prevention (DLP)

DLP aims to ensure the security of data in the cloud by preventing users from sharing sensitive or critical information with unauthorised parties. One example of a DLP system is Microsoft Purview, which works with Microsoft 365, Office, Windows, macOS and cloud apps. The administrator defines DLP policies, and the system automatically protects sensitive data using deep content analysis to detect when negligent or nefarious activity is taking place. The analysis can utilise keywords, regular expressions, function validations and secondary data matches related to a primary data match. (Microsoft, 2023)

According to Microsoft, approximately 15% of the DLP needs are geared towards protecting intellectual property. (Microsoft, 2023)

The process of implementing DLP involves the following steps:

- Identifying stakeholders, i.e., the people who can provide the following information:
- Compliance policies (laws, regulations, standards) your organisation must follow
- Categories of sensitive data
- High-risk behaviour to watch for
- Priorities for protecting the data according to sensitivity
- Action to take in the event of a DLP policy match
- Describing the categories of sensitive data
- Setting objectives
- Creating an implementation plan
- Discovering sensitive data
- This can be carried out using existing metadata, such as sensitivity labels or tags
- It may also take the form of a full data audit
- Creating and deploying policies

For the deployment, Microsoft gives the example of a small business that wants to protect its intellectual property. The recommended steps are as follows:

- Use the default DLP policy in Teams
- Set SharePoint to restrict by default
- Use policies to prevent external sharing
- Deploy policies on Windows computers
- Block uploads to cloud storage other than Microsoft OneDrive (Microsoft, 2023)

10.3 Security Information and Event Management (SIEM)

SIEM solutions use various techniques to analyse log and event data with the aim of detecting threats. One example of such a service is Splunk, which uses machine learning and custom detection methods to identify threats based on a number of widely-used frameworks, such as MITRE ATT&CK. Splunk integrates with AWS, Google Cloud, Azure and various other technologies. (Splunk, 2023)

10.4 Reference architectures

Several reputable organisations provide reference security architectures, including the following:

- Cisco Security Reference Architecture (Cisco, 2023)
- AWS Security Reference Architecture (AWS Professional Services Team, 2022)
- Azure Reference Architectures for multiple use cases (Microsoft, 2023)

- Google Cloud security foundations guide (Google, 2022)
- US Cybersecurity and Infrastructure Security Agency (CISA) cloud security technical reference architecture (Cybersecurity and Infrastructure Security Agency, 2021)
- IBM security architecture for cloud applications (IBM, 2023)

The exact security architecture required for each organisation and use case is strongly dependent on the nature of the use case. For example, the security architecture needed for a web application differs from the architecture for an SAP deployment.

10.5 Orchestration services

The most popular cloud service providers (at the time of writing: AWS, Azure and Google Cloud) offer orchestration services for specific use cases. An orchestration service provisions an infrastructure capable of providing a secure deployment for the use case. Examples of such services are as follows:

- AWS Elastic Beanstalk
    - An infrastructure consisting of the following:
        - Compute power (EC2 instances) with auto-scaling
        - Storage (S3 buckets)
        - Database (RDS)
- AWS Lightsail
    - A website and web app deployment platform with pre-configured cloud resources
- Azure App Service
    - An infrastructure for web apps, consisting of the following:
        - Compute power
        - Storage blob
        - Azure SQL database
        - Azure Web Application Firewall
- Google Cloud App Engine
    - An infrastructure for hosting web apps that can “scale to zero”
    - Includes the following services:
        - Compute
        - Storage
        - SQL

All of the above also provide management consoles, dramatically simplifying the task of infrastructure management. In contrast with a conventional cloud deployment, where each component must be provisioned and configured individually, an orchestration service utilises the cloud service provider’s best practices to offer a package that should operate sufficiently securely “out of the box”. However, orchestrated services can also be misconfigured, so they are not guaranteed to be secure.

11 Results

The report has covered the key areas of concern for a small business that needs to protect its intellectual assets, addressing the primary research problem described in the introduction. It has also covered the sub-areas specified in the overlay matrix.

The following is a checklist of sensible measures for a small business to implement:

11.1 Legal protection

11.1.1 Registration

Registration (see section 4.1) is a means of protecting intellectual assets that meet the registration criteria. Once registered, the legislation provides for effective recourse in the event of an infringement. Registration is well-suited to intellectual assets that are likely to become or have already become public knowledge, especially brands, product designs and commercially-exploited inventions.

However, certain intellectual assets may carry value for a company but may not be eligible for registration. Computer software that does not qualify for patenting is a good example of this: it may be instrumental to the business success of a company, and if, for example, the source code became publicly available, competitors could use the knowledge to erode the company's competitive advantage and harm its business outlook. Organisations may prefer to preserve such assets as trade secrets.

In this domain, it is difficult to recommend a single course of action applying to all micro and small enterprises. The necessity of registration depends heavily on the nature of the organisation's assets.

11.1.2 Trade secrets

The legislation on trade secrets (see section 4.2) is useful for protecting intellectual assets that cannot be registered as other forms of intellectual property, such as patents. Other advantages include the fact that there is, naturally, no disclosure obligation for trade secrets and, as long as the secret is not disclosed, no limit to the period of protection. In contrast with a patent, which becomes public knowledge and can be freely exploited after expiry, a trade secret can be kept indefinitely. The classic example of this is the recipe for Coca-Cola (Searle, 2021), which is kept in a secure vault in the USA and is only known to a few people in the world (Coca-Cola, 2023).

The disadvantages are that the protection of trade secrets is weaker than the protection of patents. For example, the Finnish Trade Secrets Act specifically excludes the acquisition of trade secrets from protection if it results from:

- Independent creation or discovery
- Study, disassembly, testing or observation of a product made available to the public
- Exercises of the rights of employees and their representatives to gain information
- Other practices included in “honest commercial practices” (Finlex, 2018)

Therefore, it is legal under trade secrets legislation to reverse-engineer a product or independently create a substantially similar one.

A further disadvantage to a reliance on trade secret protection is that once a trade secret is publicly disclosed, it ceases to be a trade secret according to the European Union definition described in section 4.2.

For a micro or small enterprise, a reliance on trade secrets may be an economical approach to protecting intellectual assets. It enables the organisation to avoid the complexity and expense of registration processes, which may involve submitting applications in many separate jurisdictions, and it can provide very long-lasting protection of intellectual assets. For example, Coca-Cola was invented in 1886, and the recipe remains a secret (Coca-Cola, 2023).

11.1.3 Legal recourse

Section 4.3 covers some of the aspects of restitution in the event that registered intellectual property or trade secrets are misappropriated. However, the theoretical background would imply that a malicious competitor could benefit from working under the ethos that “it is easier to gain forgiveness than permission”. Figure 5 shows three potential outcomes of legal action following the misappropriation of intellectual assets. M stands for a malicious actor, and RO stands for the rightful owner of the intellectual property.

Before any outcome is reached, RO must embark on the arduous process of bringing legal action against M, including the potential for high legal expenses. Two of the potential outcomes result in M continuing to use RO’s intellectual assets, although RO may never have intended to license them to other parties. Even in the case where RO is awarded damages, the theory indicates that the award may be insufficient to cover the actual harm caused by M and may, in any case, be difficult to recover from M, especially in the event of bankruptcy.

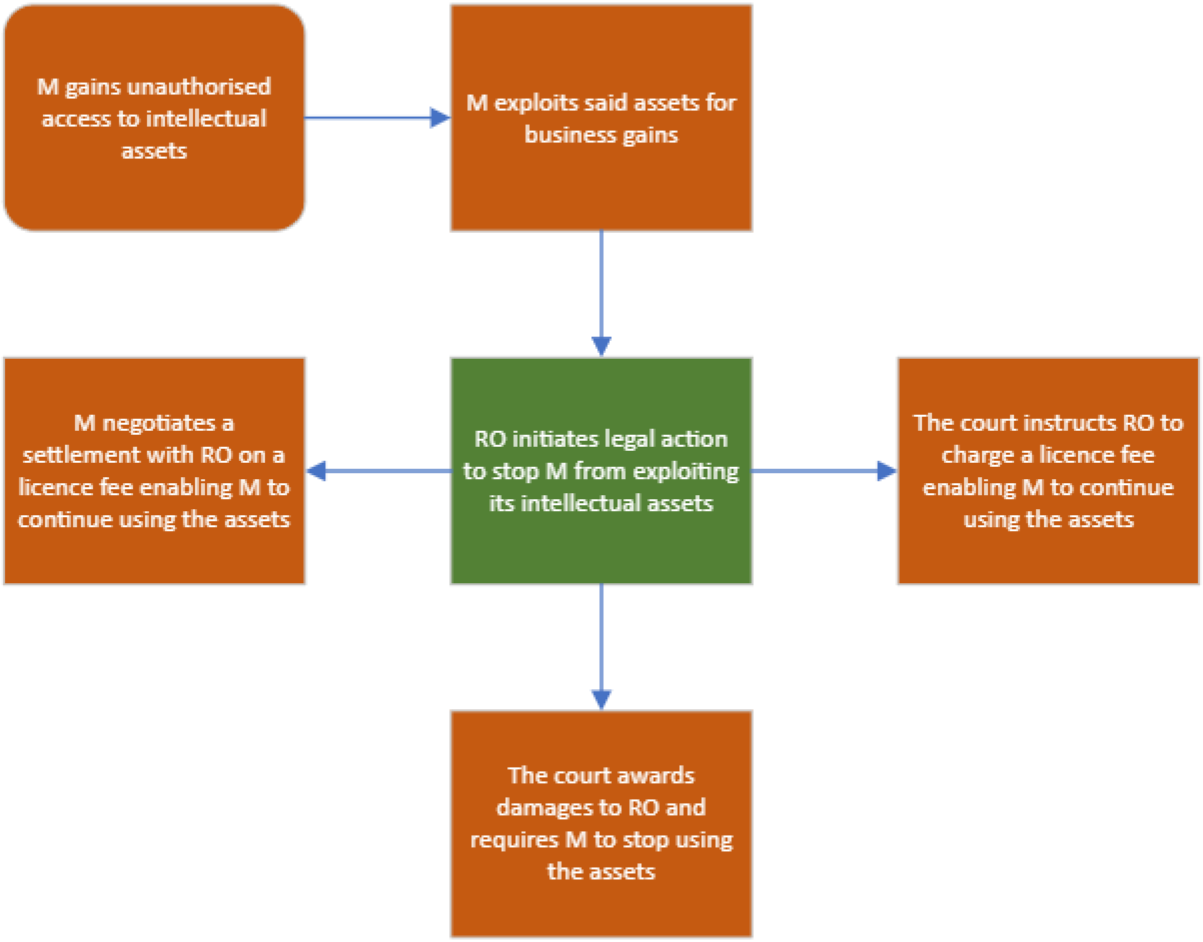

M gains unauthorised access to intellectual assets
M exploits said assets for business gains
M negotiates a settlement with RO on a licence fee enabling M to continue using the assets
RO initiates legal action to stop M from exploiting its intellectual assets
The court instructs RO to charge a licence fee enabling M to continue using the assets
The court awards damages to RO and requires M to stop using the assets

Figure 5. Potential outcomes of infringement actions, where M is a malicious actor and RO is the rightful owner of the intellectual property.

In the context of a micro or small enterprise, it may be preferable to avoid legal action, either by ensuring that intellectual assets are kept secret enough to prevent their exploitation by other parties or by settling disputes out of court.

11.1.4 Contractual clauses

The theory indicates that confidentiality obligations and restrictive covenants, such as non-compete clauses, may be a suitable and inexpensive avenue for micro and small enterprises looking to protect their intellectual assets. Notwithstanding concerns around enforceability, such clauses are may have a psychological effect on the employees consenting to them: unless employees are well versed in the legal intricacies of such clauses, they may inclined to comply with them for fear of incurring a substantial contractual sanction or having claims brought against them in court.

11.2 Physical and structural security

The theory indicates that all organisations, whether micro, small, medium or large, should ensure the physical security of their premises. Whether this requires significant resource expenditure depends heavily on the organisation’s premises. If the organisation needs to install a new access control system, the costs will be in the thousands of euros (Calder Security, 2023).

Micro or small enterprises could consider leasing office space in a building that provides a reception desk as part of the common service. They should also scrutinise the other physical security aspects of the building, including electronic locks, and make sure they are aware of who holds the keys to their premises.

As regards the other aspects of physical and structural security examined in section 5, the wise placement of assets within a building and selection of premises less prone to natural hazards may be entirely cost-neutral and, consequently, advisable for a micro or small enterprise looking to protect its intellectual assets.

11.3 Organisational measures

11.3.1 Employee training

The theory and standards indicate that organisations of all sizes, including micro and small enterprises, would be wise to conduct specific information security training for their employees. It should be noted that organisations may have differing internal standards on information security, so one benefit of providing security training as an aspect of the onboarding process is to standardise procedures and approaches among personnel. Such training should inform employees on how they are expected to protect the organisation’s intellectual assets.

11.3.2 Security policy

The theory indicates that organisations should define document sensitivity levels (see section 6.2.1) and draw up policies in the following areas:

- Classification of information
- Removal rights for intellectual assets
- Hybrid work

As regards access rights, organisations should follow the Principle of Least Privilege, granting a user only the access rights that are essential for performing their legitimate duties.

Organisations should also have an offboarding policy, preferably including a documented procedure for revoking an outgoing employee’s access to all the organisation’s data. To this end, the organisation should keep an up-to-date record of the applications and systems to which access rights are granted. The organisation should also not forget to require outgoing employees to return physical keys and other access passes to the premises.

These steps combat the potential for ex-employees to access an organisation’s intellectual assets without authorisation and, potentially, misuse them.

11.3.3 Hybrid work

Employees embarking on hybrid work should be provided with appropriate training in the ground rules for maintaining security while working remotely. The training should cover the organisation’s policies on using computing hardware outside the office (see section 6.1), removal rights (see section 6.2.2), the permitted applications (see section 7.2), working in secure places, and the network security measures required outside the office (see section 9.4).

Employees should not be permitted to work on sensitive data in public places where the data could be exposed to third parties via eavesdropping or theft. The prohibition should apply to sensitive data in all forms:

- Paper copies
- Documents opened on the screens of computers, tablets and other devices
- Messages, including email and instant messaging
- Video, including videoconferences
- Audio, including phone calls
- Physical models, such as 3D-printed prototypes

In principles, organisations should be concerned about their assets being in any places where third parties could come into close proximity to their employees or assets. Places where privacy may be limited or non-existent include coffee shops, libraries, parks and open-plan coworking spaces. The latter may be a particular concern for the organisation if the coworking space resembles the organisation’s own office, causing employees to “let their guard down” in such an environment. Indeed, a study by Clutch found that 23% of employees using coworking spaces identified security and safety concerns as key challenges in such an environment (Herhold, 2022).

11.4 Software security

11.4.1 Authentication security

The theory indicates that it would be preferable to require users to use a password management application to generate and store random secure passwords for their various accounts. Such software should not be a major financial burden on a micro or small business. For example, the business edition of LastPass costs €5.70 per user per month.

However, if the organisation does not find it appropriate to use a password manager, the theory indicates that the organisation should require users to have passwords satisfying these main criteria:

- Minimum length: 12 characters
- Do not truncate passwords when hashing/storing them
- Ensure that pasting is allowed
- Do not enforce password rotation
- Compare passwords against a blacklist of passwords that are not allowed
- Require passwords to be reset if a password leak occurs

The theory also indicates that organisations should use multifactor authentication, which should be possible without great expense to the organisation.

Secure authentication policies help to protect the organisation's intellectual assets by denying access to unauthorised users and making it difficult for them to infiltrate the accounts of legitimate users.

11.4.2 Software standardisation

If possible, the organisation should require users to use standard software. This helps the organisation to understand the security risks of each application. A centralised software provisioning and management tool, usually the preserve of larger organisations, could also be used by micro and small enterprises to control the software employees are allowed to use.

Mandating standardised software helps the organisation to control access to its intellectual assets. For example, in the absence of a standardised palette of software, a user may choose to use an application that automatically backs up edited documents to the software provider's cloud service – a potentially undesirable outcome in terms of protecting the company's intellectual assets.

11.4.3 Anti-malware

Organisations should mandate anti-malware software, using Windows Defender at a minimum for Windows computers.

11.4.4 Encryption

The theory indicates that micro and small organisations should encrypt the storage devices of workstations and network traffic in transit (via TLS/HTTPS). Passwords should undergo one-way encryption (hashing) to render it impossible to access the original password in the event of a data breach.

11.5 Hardware security

11.5.1 Filters and locks

If the organisation chooses to permit its employees to work in public places, such as coffee shops, it would be wise to mandate the use of privacy filters and physical locks, such as Kensington Locks, if the place offers anchoring points.

From a business perspective, the challenge of physical locking is to ensure that anchoring points are available where they are needed. The most compelling application for a physical lock is when a device needs to be left unattended in a public place – for example, when using the toilet at a coffee shop or if a device is present in the company's public premises, such as a shop. In other common work settings, physical locks may be of less value.

11.5.2 Biometric security

Considering the effectiveness of biometric security, as borne out by the research in section 8.3, micro and small enterprises would be wise to mandate the use of biometric security to access the operating systems of workstations, whether by requiring the use of an integrated fingerprint reader or relying on a software solution, such as Windows Hello. In both cases, the deployment of biometric security requires no additional capital investment.

11.5.3 Hardware encryption

The theory indicates that micro and small enterprises would be wise to use hardware encryption. If the workstations are Apple devices, such encryption is included in the hardware. Otherwise, a self-encrypting drive can be selected without incurring dramatic additional expense.

11.5.4 End of lifecycle

Environmentally-minded companies may be uninclined to destroy decommissioned storage media that is still in a useable state. If this is the case, the company would be well advised to securely erase all the data on the media, as described in section 8.5, when it is taken out of use.

A micro or small enterprise could risk losing control of its intellectual assets if an outside party could recover them from an old storage device.

11.6 Network security

The theory suggests that organisations of all sizes should make effective use of firewalls and segmentation in their networks. In line with the Zero Trust Model, they should treat all network traffic as suspicious and protect as many exposed attack surfaces as possible. This helps to prevent the risk of a company's intellectual assets from being stolen by an attacker who has compromised a different network appliance.

The theory highlights a risk for companies offering virtual private network (VPN) connections to their employees (see section 9.4) and indicates that VPN-less application access, including cloud-native applications, or Desktops as a Service (DaaS) would be preferable in terms of minimising the potential for intrusion and the loss of intellectual assets.

A cost-effective way for a micro or small enterprise to take such a step would be to use the cloud-native alternatives of software that is otherwise installed locally. For example, Microsoft 365 allows Microsoft's popular office applications to be used via a web browser. Consequently, the organisation should incur no additional licensing fees for using this approach. For more specialised software with no cloud-native implementations, organisations would be wise to consider the merits of DaaS, although cost may be a barrier to the selection of such an approach.

11.7 Cloud security

According to the theory, a micro or small enterprise that needs a secure cloud service has two sensible options to prevent unauthorised access to its intellectual property:

11.7.1 Manual configuration according to reference architectures

If the organisation has an employee with cloud expertise, they could construct a secure cloud architecture by consulting the reference architecture from the cloud service provider. The theory indicates that they would be wise to include identity and access management, data loss prevention, and security information and event management.

11.7.2 Orchestration

For organisations that lack in-house expertise on cloud security, an orchestration service would provide a better alternative for creating a secure cloud environment.

12 Conclusion

Micro and small enterprises would be well advised to take the following measures as a checklist for protecting their intellectual assets:

12.1 Legal protection

- Either:
    - Register all eligible assets and inventions to provide legal recourse in the event that they are misappropriated and exploited (section 4)
- Or:
    - Take all necessary measures to ensure that intellectual assets remain secret and fulfil the criteria of a trade secret (section 4.2)
- Take legal action in the event of an intellectual property infringement (section 4.3)

12.2 Physical security

- Ensure your premises are built in a way that prevents unauthorised parties from gaining access to intellectual assets (section 5)
    - Use access control (section 5.2)
    - Use an intruder detection and alarm system (section 5.3)
- Place the most valuable assets securely within the building (section 5.4)

12.3 Organisational security

- Provide employees with security training (section 6.1)
- Have security policies covering at least the following areas:
    - Classification of information (section 6.2.1)
    - Asset removal rights (section 6.2.2)
    - Regular reviews of access rights (section 6.2.3)
    - Offboarding policy for departing personnel (section 6.2.4)
- If you allow hybrid work, make sure you have a security policy for it:
- Ground rules (section 6.3)
- Policy on where hybrid work is permitted (section 6.3)

12.4 Software security

- Manage authentication securely (section 7.1)
- Use complex password rules (section 7.1.1)
- Require personnel to use password managers (section 7.1.2)
- Enforce multifactor authentication (section 7.1.3)

- Use standardised software within the organisation or Desktops as a Service (section 7.2)
- Use anti-malware software (section 7.3)
- Enforce encryption (section 7.4)
  - Software encryption of storage devices (BitLocker or equivalent, section 7.4.1)
  - Encrypted communications (section 7.4.2)
  - Web traffic
  - Instant messages
  - Online calls
  - Emails, if necessary
- One-way hashes for storing passwords and other sensitive data (section 7.4.3)
- Refer to security frameworks such as OWASP when developing software products (section 7.5)

12.5 Hardware security

- Use privacy filters to protect on-screen information (section 8.1)
- Use locks to secure laptops and other suitable devices (section 8.2)
- Use biometric security as an additional factor in authentication (section 8.3)
- Choose self-encrypting hardware (section 8.4)
- Have an end-of-lifecycle policy for storage media (section 8.5)

12.6 Network security

- Design your network to allow for microsegmentation and the Zero Trust Model (sections 9.2 and 9.3)
- Use next-generation firewalls as segmentation gateways (section 9.1.3)
- Supplement hardware/virtual hardware firewalls with software firewalls, such as Microsoft Defender (section 9.1.4)
- Create and enforce a policy on network security in a hybrid work environment (section 9.4)
  - VPN
  - Secure VPN-less access
  - Desktop as a Service

12.7 Cloud security

- Create cloud versions of the network security infrastructure referred to above
- Deploy effective identity and access management for cloud resources (section 10.1)
- Deploy a data loss prevention solution (section 10.2)
- Use security information and event management to detect and track abnormal network access (section 10.3)

- Compare your deployment with a reference architecture (section 10.4)
- Use orchestration services if they are compatible with your organisation’s workloads and budget (section 10.5)

These checklists are summarised in the security cube in Appendix 1. The purpose of the security cube is to serve as an almost playful item that a manager of a small business could keep on their desk as a visual reminder of the security measures referred to in this report.

13 Discussion

The complex palette of measures is intended to provide all-round protection for a small organisation's intellectual assets. In practice, many of the steps referred to above may not require a concerted effort while others may be handled by third parties. Nonetheless, it is important for the organisation to be aware of its options and protections.

The following are some examples:

- Copyrights arise automatically and do not need to be registered (section 4.1.1). Similarly, trade secrets are protected, provided that the criteria of novelty, secrecy and protection are satisfied (section 4.2).
- In leased premises, the physical security actions referred to in section 12.2 may be the responsibility of the lessor or landlord.
- Employee training could be outsourced.
- The default security settings of software such as Microsoft Defender offer good protection (section 9.1.4).
- The orchestration services offered by cloud service providers make it easy to provision the cloud infrastructure required for a secure deployment of an application or website (such as AWS Elastic Beanstalk, AWS Lightsail, Azure App Service or Google Cloud App Engine)

The results of this research are, by their nature, relevant to a certain point in time. They concern areas of technology that are rapidly evolving. As such, further developments in this area could focus on updating the recommendations and analysing the relevance of the existing recommendations.

This research is mainly based on documented facts on the law, regulation, procedures and technical functioning of systems. The sources referred to are authoritative, being the authorities concerned and the owners of the systems and solutions in question. The research does not have any specific ethical questions. The results are readily reproducible with reference to the official publications from the organisations concerned. They could be expanded upon by seeking similar information from other organisations. For example, the steps required to configure a secure cloud hosting environment with a provider other than AWS, Azure or Google are likely to be published by the relevant cloud service provider.

In terms of future research, it may be enlightening to conduct a survey of businesses to discover their experiences with information security in the early stages of their operations. However, it may be challenging to identify companies willing to divulge potentially sensitive information, especially if they have suffered negative consequences due to inadequate information security.

In conducting this research, I have learned a lot about the security challenges facing the managers of micro and small enterprises. However, my approach to this thesis project should have been better organised, and I should have consulted with my supervisor more frequently. These are important lessons I will take with me into future studies.

14 References

3M. (2023, April 17). *Privacy and Screen Protectors.* Retrieved from 3M: https://www.3m.com/3M/en_US/privacy-screen-protectors-us/

Almeling, D. S., Snyder, D. W., Sapoznikow, M., McCollum, W. E., & Weader, J. (2009). A Statistical Analysis of Trade Secret Litigation in Federal Courts. *Gonzaga Law Review*, 291-334.

Apple. (2022, April 27). *Apple Business Manager User Guide.* Retrieved from Apple Support: https://support.apple.com/en-gb/guide/apple-business-manager/axmd344cdd9d/web

Apple Computer. (2022, April 27). *About Face ID advanced technology.* Retrieved from Apple Support: https://support.apple.com/en-us/HT208108

ASSA ABLOY. (2021, November 1). *ASSA ABLOY has grown to secure homes and businesses worldwide.* Retrieved from ASSA ABLOY: https://www.assaabloy.com/group/en/news-media/stories/access-stories/assa-abloy-has-grown-to-secure-homes-and-businesses-worldwide

Attorney General of Texas. (2018, September 26). *AG Paxton Reaches $148 Million Settlement with Uber for Data Breach.* Retrieved from Attorney General of Texas: https://www.texasattorneygeneral.gov/news/releases/ag-paxton-reaches-148-million-settlement-uber-data-breach

Autoriteit Persoonsgegevens. (2018, November 27). *Dutch DPA: fine for data breach Uber.* Retrieved from Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber

AWS. (2017). *Security in the Cloud: A Checklist for Cloud Buyer.* Retrieved from AWS: https://community.spiceworks.com/partners/content/aws-security-checklist

AWS Professional Services Team. (2022, December). *AWS Security Reference Architecture (AWS SRA).* Retrieved from Amazon Web Services: https://d1.awsstatic.com/APG/aws-security-reference-architecture-v3.pdf

Calder Security. (2023, May 24). *How much do access control systems cost?* Retrieved from Calder Security: https://www.caldersecurity.co.uk/access-control-systems-cost/

Chesnut, R. (2022, October 12). *Uber Security Chief's Conviction Raises Red Flags: Good Counsel.* Retrieved from Bloomberg Law: https://news.bloomberglaw.com/business-and-practice/good-counsel-uber-security-chiefs-conviction-raises-red-flags

Cisco. (2023, March 18). *Security Reference Architecture.* Retrieved from Cisco.com: https://www.cisco.com/go/sra

Cisco. (2023, April 13). *Small Business Network Security Checklist.* Retrieved from Cisco.com: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/security/network-security-checklist.html

Cisco. (2023, April 13). *What is a firewall?* Retrieved from Cisco.com: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html

Cisco. (2023, April 14). *What is a next-generation firewall?* Retrieved from Cisco.com: https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

Clark, D. S. (2017). *Complaint in the matter of Uber Technologies Inc.* Retrieved from Federal Trade Commission: https://www.ftc.gov/system/files/documents/cases/1523054_uber_technologies_complaint.pdf

Coca-Cola. (2023, May 24). *Who knows the secret formula of Coca-Cola?* Retrieved from Coca-Cola Great Britain: https://www.coca-cola.co.uk/our-business/faqs/who-knows-the-secret-formula-of-coca-cola

Cybersecurity and Infrastructure Security Agency. (2021, August). *Cloud Security Technical Reference Architecture.* Retrieved from CISA.gov: https://www.cisa.gov/sites/default/files/publications/CISA%2520Cloud%2520Security%2520Technical%2520Reference%2520Architecture_Version%25201.pdf

Cybersecurity Insiders. (2021). *BYOD Security Report.* Retrieved from Bitglass: https://pages.bitglass.com/rs/418-ZAL-815/images/CDFY21Q2BYOD2021.pdf

Denham, E. (2018, November 26). *Monetary Penalty Notice.* Retrieved from Information Commissioner's Office: https://ico.org.uk/media/action-weve-taken/mpns/2553890/uber-monetary-penalty-notice-26-november-2018.pdf

Diamond, P. (2020, September 8). *10 tips to protect your files on your PC and in the Cloud.* Retrieved from Microsoft Business Insights and Ideas: https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/10-tips-to-protect-your-files-on-pc-and-the-cloud

Directorate-General for Communications Networks, Content and Technology. (2022, July 25). *Copyright.* Retrieved from Shaping Europe's digital future: https://digital-strategy.ec.europa.eu/en/policies/copyright

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs. (2013, July 12). *Study on trade secrets and confidential business information in the internal market.* Retrieved from European Commission Publications: https://single-market-economy.ec.europa.eu/publications/study-trade-secrets-and-confidential-business-information-internal-market_en

Eur-Lex. (2004, April 29). *Directive 2004/48/EC of the European Parliament and of the Council.* Retrieved from Eur-Lex: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0048R(01):EN:HTML

Eur-Lex. (n.d.). *Regulation (EU) 2017/1001 of the European Parliament and of the Council.*

European Commission. (2023). *Copyright.* Retrieved from IP Helpdesk: https://intellectual-property-helpdesk.ec.europa.eu/copyright_en

European Observatory on Counterfeiting and Piracy. (2009). *Injunctions in Intellectual Property Rights.* Retrieved from EUIPO: https://euipo.europa.eu/ohimportal/documents/11370/80606/Injunctions+in+Intellectual+Property+rights

European Observatory on Counterfeiting and Piracy. (2010). *Damages in Intellectual Property Rights.* Retrieved from EUIPO: https://euipo.europa.eu/ohimportal/documents/11370/80606/Damages+in+intellectual+property+rights/b0d70979-2af3-48cf-870b-9ed1139d917a

European Parliament and Council. (2016, June 15). *Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Text with EEA relevance).* Retrieved from Eur-Lex: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0943

European Patent Office. (2000, November 29). *Convention on the Grant of European Patents (European Patent Convention).* Retrieved from European Patent Office: https://www.epo.org/law-practice/legal-texts/html/epc/2016/e/EPC_conv_20200701_en_20200620.pdf

European Patent Office. (2023). *FAQ - applying for a patent.* Retrieved from European Patent Office: https://www.epo.org/service-support/faq/own-file.html

European Patent Office. (2023). *Guidelines for Examination.* Retrieved from European Patent Office: https://www.epo.org/law-practice/legal-texts/html/guidelines/e/g_ii_3_6.htm

European Union Intellectual Property Office. (2023). *Trade marks basics.* Retrieved from European Union Intellectual Property Office: https://euipo.europa.eu/ohimportal/en/trade-marks-basics

Eurostat. (2022, November 8). *Rise in EU population working from home.* Retrieved from Eurostat: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/ddn-20221108-1

Eurostat. (2023, May 24). *Small and medium-sized enterprises (SMEs).* Retrieved from Eurostat: https://ec.europa.eu/eurostat/web/structural-business-statistics/information-on-data/small-and-medium-sized-enterprises

Federal Communications Commission. (2023). *Cybersecurity for Small Businesses.* Retrieved from Federal Communications Commission: https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses

Federal Trade Commission. (2018, April 25). *Analysis of Proposed Consent Order to Aid Public Comment in the Matter of Uber Technologies, Inc., File No. 1523054.* Retrieved from Federal Trade Commission: https://www.ftc.gov/system/files/documents/federal_register_notices/2018/04/152_3054_uber_revised_consent_analysis_pub_frn.pdf

Federal Trade Commission. (2023, January 5). *Non-Compete Clause Rulemaking.* Retrieved from Federal Trade Commission: https://www.ftc.gov/legal-library/browse/federal-register-notices/non-compete-clause-rulemaking

FIDO Alliance. (2023, March 29). *FIDO2: Web Authentication (WebAuthn).* Retrieved from FIDO Alliance: https://fidoalliance.org/fido2-2/fido2-web-authentication-webauthn/

Finlex. (1999, September 30). *Land Use and Building Act.* Retrieved from Finlex: https://www.finlex.fi/en/laki/kaannokset/1999/en19990132

Finlex. (2018). *Trade Secrets Act, 595/2018.* Retrieved from Finlex: https://finlex.fi/en/laki/kaannokset/2018/en20180595

Finlex. (2019, February 5). *Employment Contracts Act.* Retrieved from Finlex: https://www.finlex.fi/en/laki/kaannokset/2001/20010055

Finlex. (2022, December 7). *Criminal Code.* Retrieved from Finlex: https://www.finlex.fi/en/laki/kaannokset/1889/en18890039

Finnish Patent and Registration Office. (2019, June 11). *What kind of inventions can get utility models?* Retrieved from Finnish Patent and Registration Office: https://www.prh.fi/en/hyodyllisyysmallit/theabcofutilitymodels/whatkindofinvention.html

Finnish Patent and Registration Office. (2023). *What kind of inventions can be patented?* Retrieved from Finnish Patent and Registration Office: https://www.prh.fi/en/patentit/theabcofpatenting/whatcanbepatented.html

Global Cyber Alliance. (2023). *GCA Cybersecurity Toolkit for Small Business Handbook.* Retrieved from GCA Cybersecurity Toolkit: https://gcatoolkit.org/smallbusiness/

Google. (2022, December). *Google Cloud security foundations guide.* Retrieved from Google: https://services.google.com/fh/files/misc/google-cloud-security-foundations-guide.pdf

Grassi, P. A., Fenton, J. L., Newton, E. M., Perlner, R. A., Regenscheid, A. R., Burr, W. E., . . . Theofanos, M. F. (2020, March 2). *NIST Special Publication 800-63B: Digital Identity Guidelines, Authentication and Lifecycle Management.* Retrieved from National Institute of Standards and Commerce: https://doi.org/10.6028/NIST.SP.800-63b

Griffiths, J. (2013). Constitutionalising or Harmonising? The Court of Justice, the Right to Property and European Copyright Law. *38 European Law Review*, 65-78.

Herhold, K. (2022, August 9). *Top Benefits & Challenges of Coworking Spaces.* Retrieved from Clutch: https://clutch.co/real-estate/resources/top-challenges-coworking-spaces#eleven

HP. (2023, May 25). *Securing the Hybrid Workplace in 2022 and Beyond.* Retrieved from HP: https://reinvent.hp.com/security-report

IBM. (2022, April 26). *About self-encrypting drives.* Retrieved from IBM: https://www.ibm.com/docs/en/psfa/7.2.1?topic=administration-about-self-encrypting-drives

IBM. (2023, April 18). *Security architecture for cloud applications.* Retrieved from IBM.com: https://www.ibm.com/cloud/architecture/architectures/securityArchitecture/reference-architecture

IBM. (2023, April 14). *What is cloud security?* Retrieved from IBM: https://www.ibm.com/topics/cloud-security

International Organization for Standardization. (2013). *International Standard ISO/IEC 27002.* Geneva: International Organization for Standardization.

International Organization for Standardization. (2022, October). *ISO/IEC 27001:2022.* Retrieved from ISO.org: https://www.iso.org/standard/82875.html

Johns, E. (2021, March 24). *Cyber Security Breaches Survey 2021.* Retrieved from Gov.UK: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Kaspersky. (2023, April 14). *Next Generation Firewall (NGFW).* Retrieved from Encyclopedia by Kaspersky: https://encyclopedia.kaspersky.com/glossary/next-generation-firewall-ngfw/

Kaspersky. (2023, April 13). *What is Unified Threat Management (UTM)?* Retrieved from Kaspersky: https://www.kaspersky.com/resource-center/definitions/utm

Kathuria, S. (2022, June 22). *Modernizing Secure Remote Access: A VPN-less Future for Hybrid Work.* Retrieved from Duo.com: https://duo.com/blog/modernizing-secure-remote-access-vpn-less-future-hybrid-work

Kensington. (2023, April 17). *Kensington.* Retrieved from Kensington: https://www.kensington.com/en-gb/p/products/security/keyed-locks/slim-nanosaver-2.0-portable-keyed-laptop-lock/

Kensington. (2023, April 18). *VeriMark™ Fingerprint Key.* Retrieved from Kensington.com: https://www.kensington.com/p/products/data-protection/biometric/verimark-fingerprint-key-fido-u2f-2nd-factor-authentication-and-windows-hello/

Khosrowshahi, D. (2017, November 21). *2016 Data Security Incident.* Retrieved from Uber Newsroom: https://www.uber.com/newsroom/2016-data-incident/

Kindervag, J. (2010). *Build Security Into Your Network's DNA: The Zero Trust Network Architecture.* Cambridge, MA: Forrester.

Kindervag, J. (2018, September 4). *Define a Protect Surface to Massively Reduce Your Attack Surface.* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/blog/2018/09/define-protect-surface-massively-reduce-attack-surface/

Kindervag, J. (2019, January 17). *You Want Network Segmentation, But You Need Zero Trust.* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/blog/2019/01/you-want-network-segmentation-but-you-need-zero-trust/

Kissel, R., Regenscheid, A., Scholl, M., & Stine, K. (2014). *Guidelines for Media Sanitization.* Gaithersburg, MD: National Institute of Standards and Technology.

Lenovo. (2023, April 18). *Lenovo Laptops.* Retrieved from Lenovo.com: https://www.lenovo.com/us/en/laptops/results?visibleDatas=860%3AFingerprint%2520Reader

Microsoft. (2022, January 11). *Use end-to-end encryption for one-to-one Microsoft Teams calls.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/microsoftteams/teams-end-to-end-encryption

Microsoft. (2022, December 9). *Windows Defender Application Control and AppLocker Overview.* Retrieved from Microsoft Documentation: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/wdac-and-applocker-overview

Microsoft. (2023, February 24). *Best practices for configuring Windows Defender Firewall.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/best-practices-configuring

Microsoft. (2023, April 18). *Browse Azure Architectures.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/azure/architecture/browse/

Microsoft. (2023, February 17). *Learn about data loss prevention.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-learn-about-dlp?view=o365-worldwide

Microsoft. (2023, March 7). *Microsoft Intune securely manages identities, manages apps, and manages devices.* Retrieved from Microsoft: https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune

Microsoft. (2023, February 17). *Plan for data loss prevention (DLP).* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp?view=o365-worldwide#plan-for-data-loss-prevention-dlp

Microsoft. (2023, February 21). *Windows Hello biometrics in the enterprise.* Retrieved from Microsoft Learn: https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/hello-biometrics-in-enterprise

Ministry of the Environment. (2023, March 27). *The National Building Code of Finland.* Retrieved from Ministry of the Environment: https://ym.fi/en/the-national-building-code-of-finland

Moberly, M. D. (2014). *Safeguarding Intangible Assets.* Butterworth-Heinemann.

Newhouse, W., Bartock, M., Ferraiolo, H., Cichonski, J., Souppaya, M., Brown, C., . . . Sexton, J. (2019). *Derived Personal Identity Verification (PIV) Credentials.* U.S. Department of Commerce.

Ocean Tomo. (2020, July). *Intangible Asset Market Value Study.* Retrieved from Ocean Tomo: https://www.oceantomo.com/intangible-asset-market-value-study/

OECD. (2018, February 22). *Promoting innovation in established SMEs.* Retrieved from OECD: https://www.oecd.org/cfe/smes/ministerial/documents/2018-SME-Ministerial-Conference-Parallel-Session-4.pdf

Olander, H., Hurmelinna, P., & Mähönen, J. (2009). What's Small Size Got to Do with It? Protection of Intellectual Assets in SMEs. *International Journal of Innovation Management*, 349-370.

Osterman Research. (2014). *Do Ex-Employees Still Have Access to Your Corporate Data?* Osterman Research.

OWASP. (2021, October). *Application Security Verification Standard 4.0.3.* Retrieved from OWASP ASVS: https://github.com/OWASP/ASVS/raw/v4.0.3/4.0/OWASP%20Application%20Security%20Verification%20Standard%204.0.3-en.pdf

OWASP. (2023, May 24). *Authentication Cheat Sheet.* Retrieved from OWASP Cheat Sheet Series: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html

OWASP. (2023, April 18). *OWASP Top Ten.* Retrieved from OWASP: https://owasp.org/www-project-top-ten/

OWASP. (2023, April 18). *Password Storage Cheat Sheet.* Retrieved from OWASP/CheatSheetSeries: https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Palo Alto Networks. (2023, April 14). *What is microsegmentation?* Retrieved from Palo Alto Networks: https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation#:~:text=Microsegmentation%20refers%20to%20an%20approach,create%20zones%20in%20cloud%20deployments.

Passman, P., Subramanian, S., & Prokop, G. (2014). *Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats.* Center for Responsible Enterprise And Trade (CREATe.org), PricewaterhouseCoopers LLP.

Pastore, R., Fuller, M., & Gillespie, J. (2022, February). *The Business Value of Migration to Amazon Web Services.* Retrieved from AWS: https://pages.awscloud.com/rs/112-TZM-766/images/hackett-group-the-business-value-of-migration-to-aws-012022.pdf

PCI Security Standards Council, LLC. (2022, March). *Payment Card Industry Data Security Standard.* Retrieved from PCI Security Standards Council: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Pinsent Masons. (2023, January 6). *Restrictive covenants in employment contracts.* Retrieved from Pinsent Masons: https://www.pinsentmasons.com/out-law/guides/restrictive-covenants-in-employment-contracts

PricewaterhouseCoopers. (2019). *Study on the scale and impact of industrial espionage and theft of trade secrets through cyber.* Retrieved from PricewaterhouseCoopers: https://www.pwc.com/it/it/publications/docs/study-on-the-scale-and-Impact.pdf

Rawlings, R. (2020, April 29). *Password Habits in the US and the UK: This Is What We Found.* Retrieved from NordPass: https://nordpass.com/blog/password-habits-statistics/

Schwartz, M. J. (2016, September 14). *Cybercrime-as-a-Service Economy: Stronger Than Ever.* Retrieved from Bankinfo Security: https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396

Searle, N. (2021, April 19). *The economic and innovation impacts of trade secrets.* Retrieved from Gov.UK: https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets

Slack. (2023, April 18). *Slack security datasheet.* Retrieved from Slack.com: https://a.slack-edge.com/964df/marketing/downloads/security/Datasheet_en-US.pdf

Smite, D., Moe, N. B., Hildrum, J., Gonzalez-Huerta, J., & Mendez, D. (2023, January). Work-from-home is here to stay: Call for flexibility in post-pandemic work policies. *Journal of Systems and Software, 195*.

Splunk. (2023, April 17). *Splunk Enterprise Security.* Retrieved from Splunk.com: https://www.splunk.com/en_us/products/enterprise-security.html

The British Standards Insitution. (2023). *The new ISO/IEC 27001:2022 standard.* Retrieved from BSI Group: https://www.bsigroup.com/en-GB/iso-27001-information-security/isoiec-27001-revision/

The Economist Intelligence Unit. (2021, May). *Open secrets? Guarding value in the intangible economy.* Retrieved from CMS Legal Services: https://cms.law/en/media/international/images/publications/exclusive-images/open-secrets/open-secrets-guarding-value-in-the-intangible-economy?v=2

Uber. (2022, September 19). *Security update.* Retrieved from Uber Newsroom: https://www.uber.com/newsroom/security-update/

Uber. (2023). *Information about 2016 Data Security Incident.* Retrieved from Uber Help: https://help.uber.com/riders/article/information-about-2016-data-security-incident?nodeId=12c1e9d1-4042-4231-a3ec-3605779b8815

United States Attorney's Office. (2022, October 5). *Former Chief Security Officer Of Uber Convicted Of Federal Charges For Covering Up Data Breach Involving Millions Of Uber User Records.* Retrieved from Justice.gov: https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-convicted-federal-charges-covering-data-breach

University of Oxford. (2020, April 7). *FBI follows Oxford academic's guide to beat the Zoom-bombers.* Retrieved from University of Oxford: https://www.ox.ac.uk/news/science-blog/fbi-follows-oxford-academics-guide-beat-zoom-bombers

Unni, A. (2022, January 11). *What You Need To Know About Crime As A Service (CaaS).* Retrieved from Stickman Cyber: https://www.stickmancyber.com/cybersecurity-blog/what-you-need-to-know-about-crime-as-a-service-csaas

World Economic Forum. (2022). *The Global Risks Report 2022 Insight Report.* Retrieved from World Economic Forum: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

World Intellectual Property Organization. (2023). *Patents.* Retrieved from World Intellectual Property Organization: https://www.wipo.int/patents/en/

World Intellectual Property Organization. (2023). *Patents.* Retrieved from World Intellectual Property Organization: https://www.wipo.int/patents/en/

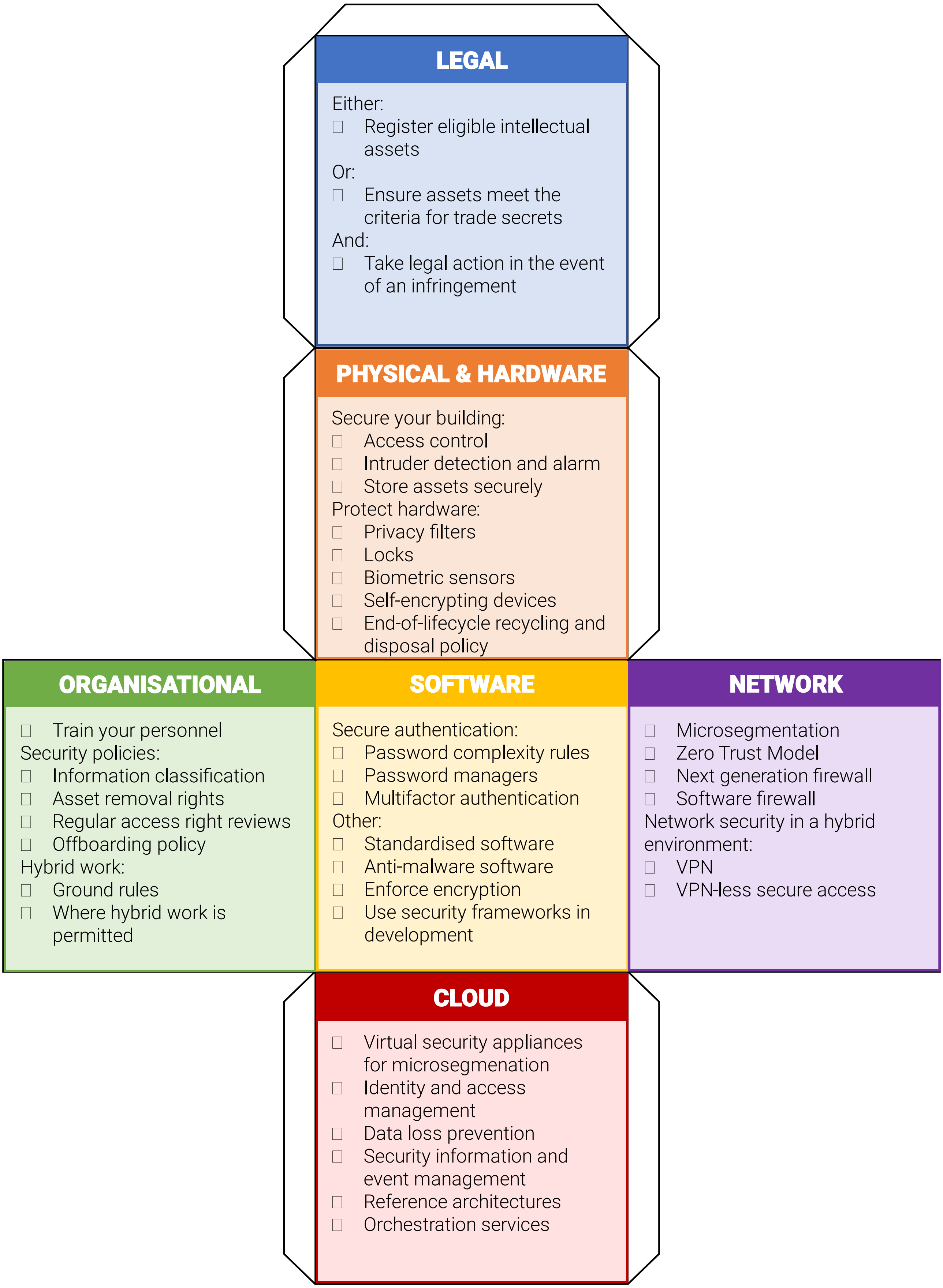
World Trade Organization. (1994, April 15). *Agreement on Trade-Related Aspects of Intellectual Property Rights.* Retrieved from World Trade Organization: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm

Your Europe. (2022, August 26). *Design protection.* Retrieved from Your Europe: https://europa.eu/youreurope/business/running-business/intellectual-property/design-protection/index_en.htm

Yuan, E. S. (2020, April 1). *A Message to Our Users.* Retrieved from Zoom Blog: https://blog.zoom.us/a-message-to-our-users/

Appendices

Appendix 1. Security cube



LEGAL

Either:
- □ Register eligible intellectual assets

Or:
- □ Ensure assets meet the criteria for trade secrets

And:
- □ Take legal action in the event of an infringement

PHYSICAL & HARDWARE

Secure your building:
- □ Access control
- □ Intruder detection and alarm
- □ Store assets securely

Protect hardware:
- □ Privacy filters
- □ Locks
- □ Biometric sensors
- □ Self-encrypting devices
- □ End-of-lifecycle recycling and disposal policy

ORGANISATIONAL

- □ Train your personnel

Security policies:
- □ Information classification
- □ Asset removal rights
- □ Regular access right reviews
- □ Offboarding policy

Hybrid work:
- □ Ground rules
- □ Where hybrid work is permitted

SOFTWARE

Secure authentication:
- □ Password complexity rules
- □ Password managers
- □ Multifactor authentication

Other:
- □ Standardised software
- □ Anti-malware software
- □ Enforce encryption
- □ Use security frameworks in development

NETWORK

- □ Microsegmentation
- □ Zero Trust Model
- □ Next generation firewall
- □ Software firewall

Network security in a hybrid environment:
- □ VPN
- □ VPN-less secure access

CLOUD

- □ Virtual security appliances for microsegmenation
- □ Identity and access management
- □ Data loss prevention
- □ Security information and event management
- □ Reference architectures
- □ Orchestration services