

Study Skills assignment FINAL

Aaron Bell

by Aaron Bell

Submission date: 13-Jan-2025 12:56PM (UTC+0000)

Submission ID: 248246999

File name: 59334_Aaron_Bell_Study_Skills_assignment_FINAL_Aaron_Bell_632112_1669562670.docx (1.25M)

Word count: 4414

Character count: 24849

Study skills for Electronics ACDA4021

Embedded Electronics L6 Degree
Apprenticeship

By Aaron Bell (2410529)

1.0 Presentation

The author of the report describes themselves as having a professional background in Cyber Security and Network Engineering, demonstrating a technical pathway and development towards what the author later describes as a long term goal of achieving an MSc in Cyber Security and Cisco Certified Internetwork Expert qualifications. The author considers themselves to be quite introverted, taking up hobbies such as Chess and Amateur radio that don't directly involve social situations or having a great deal of direct interaction with other people.

They list their weaknesses as

- Dealing with people.
- Being overcritical of themselves.
- Shutting off quickly when looking at topics they don't enjoy.

Key points the author feels they have learned from trying to produce the above PowerPoint presentation are as follows:

- There was little to no documentation of the author's life, a complete lack of photos perhaps in the future more should be done to allow for a generic about me in future presentations that may be given to the public or general technical audiences outside of employment.
- The author describes experience of giving technical presentations, with those presentations often including some interactivity with the audience. In the future it might be relevant to include such sections in smaller presentations to maintain audience engagement with the presenter.
- It remains difficult for some individuals, particularly introverts to discuss at length; details about themselves. Perhaps brainstorming will work as a more effective technique for planning a presentation like the one given by the author in the future.

Upon reflection from feedback from peers, the author believes three key things may improve similar presentations in the future:

- Go into more detail about hobbies, since they are a significant part of the author's life.
- Speak more appropriately and consideration of alternative words where required.
- Include images for the audience to look at and to reference hobbies and background.

Screenshots from the presentation that is described above may be found in Annex A.

2.0 Personal Research on required skill sets

2.1 Skills required for successful learning in a Higher Education environment

Adaptive thinking, critical thinking and problem solving [1], are listed frequently as being key skills for success in both studies and in employability. These skills are important for solving problems and adapting to ever changing environments that the author may find themselves in. The author actively works on these skills through their hobbies of chess, programming and network configurations.

Motivation [2] is listed as another key skill for successful studies, since a lot of study, especially in the later years will be self-directed and having a strong motivation will make it far easier to manage time and workload independently.

2.2 Skills that employers look for in prospective job candidates.

Employers not only want employees with domain specific knowledge in areas such as STEM (Science, Technology, Engineering and Mathematics), but also transferable skills, many of which are also required for success at university like critical thinking and problem solving.

Soft skills are one of the most important aspects of a successful career, some examples of these soft skills include: Communication, Leadership, Positivity and Flexibility [3].

Figure 1 shows results from the National careers service skills assessment [4].

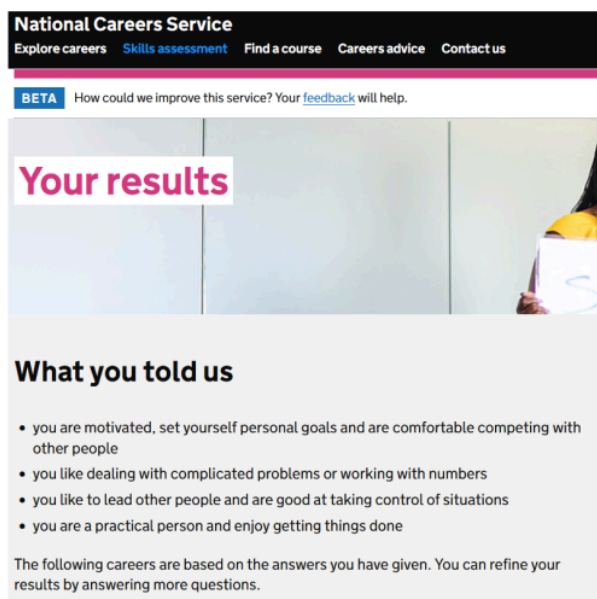


Figure 1 - National Careers Centre Skills Assessment

The skills assessment gives results on the author's answers to agree/disagree questions, whilst this doesn't directly show soft skills, it allows for the author to understand the best ways in which those skills can be developed and what they are comfortable with. These results also align very well with a career in science and technology.

Employers view soft skills as even more important to work readiness. [5] This is likely because these soft skills are much harder to train than hard technical skills, those with strong soft skills will become much more effective employees and team members, regardless of their technical ability at that moment in time. This couples with an eagerness to learn, and passion for a subject... it's slightly cloudy where these skills lie, however they are two things that an individual either has, or doesn't and will be absolutely critical to success in a technical career.

3.0 Self-evaluation and action planning

The main goals of the author are listed below:

- Achieve CCNP in preparation for the future goal of obtaining a CCIE.
- Complete the first year of university and achieve over 60% on their assignments.
- Complete the process of earning a promotion with their employer and going up a level.
- The author would like to achieve 1800+ ELO rating in chess online and 1500+ ECF over the board rating within the next year.

A key professional goal of the author is to attain their Cisco Certified Network Professional qualification during the course of 2025/2026, the author recently built a business case for this qualification as has been given funding to go ahead and train. It will be achieved by completing the ENCOR exam and lab exercises, followed by a specialisation exam of either "planning wireless networks" or "service provider networks". With ENCOR to be sat in late 2025 and the specialisation to follow depending on success in the previous exam, as both are required to hold CCNP.

The author took a number of personality tests as a result of this assignment, the full results are shown in Annex B. However two of these results, one from the Fisher Temperament Inventory and the other from the Myers-Briggs Personality test demonstrate the following results: Analytical/Tough-Minded temperament and a personality type of INTJ. It is quite surprising how well this appears to match the author, by looking at the author's history of chess games, aggression and intuition are two recurring themes. It has been said that the way a player plays chess, will reflect elements of their personality; clearly demonstrated here.

Finally, reflecting on the author's personality test, careers matches for architects, engineers and physicists are fitting and accurate as the author is currently working as an engineer for Dstl. With further aspirations to develop as a network engineer and in the long term go on to become a network architect.

Annex C contains SMART goals set by the author.

4.0 Application

4.1 Looking after your data

Looking after data comes in two parts for academic purposes. Utilizing the CIA triad [6], for purposes of considering information in this context, both integrity and availability are forefront, with confidentiality taking a backseat for most personal academic information unless specific to research.

Integrity means that the information remains whole, and unedited. A student needs to ensure that the information cannot be changed by anyone else, this would lead a failure in academic context but also applies to protection from malware and corruption.

Availability refers to the ability to access information, be it digital files or physical documents in a timely manner. Crucial to ensuring that assignments can be submitted on time and that information is held in a safe place that is known and easy to access.

The author uses three points to store data, one online and two offline copies are held. Online copies are held in cloud storage and offline copies are held on personal computer and removable media devices. This ensures that if one source is not available, that there are other up to date copies of the information required. A point to be improved is syncing documents between the computer and removable media, which is something the author will seek to configure in the near future.

The author also is aware that when integrity of a file is heavily required, that using sha256sum or Get-FileHash is likely the best way to ensure files remain unedited,

recording and checking the file hash ensures that the file was not changed, even if it has been renamed.

The author has decided not to include a directory structure in this document, the specifics of how files are stored is something left up to the choice of the individual, and may not make sense to other persons. So long as this structure remains coherent and the person using it knows how to navigate and find the information they need, that is the most important part.

4.2 Time management and self-organisation

Management of your time, particularly when working full-time and doing a part-time degree is incredibly important. Such as in the authors case, where dedicated time has to be set aside for completing university work and reading. Gratefully, the author's employer allows for one day a week (7.4 hours) to be dedicated to studying for university and completing assignments.

Outside of this situation, the author uses a proprietary time planner/schedule manager to keep organised and aware of what tasks they have planned for each day of the week, similar to a technique known as calendar blocking but in a more interactive format. Shown in Annex D is the authors schedule for the week using the app ME+. Whilst the author doesn't strictly adhere to this every day, it allows for easier planning of additional events that pop up, since a source of knowing what the authors commitments are on a particular day allows them to ensure things do not overlap.

Whilst tangentially related to time management, self-organisation applies in many areas of academic life, since there are times where independent working is required, meaning nobody is going to be on your back about getting things done. This requires you to be prepared, self-motivated and organised to balance both life and meeting the requirements of tasks such as independent projects.

Self-organisation can also be seen as relevant to both digital and physical environments, where ensuring that you have clean and safe workspaces where you can focus to the best of your ability and get tasks done. As well as keeping digital devices away from distractions as much as possible when you are working towards a deadline.

5.0 Conclusion and Evaluation

The author has set themselves achievable goals in order to progress academically, professionally and within their hobbies. Whilst these goals are difficult, so long as they are worked towards and progress is made, the timelines can be moved slightly to allow for potential complications that have been foreseen by the author and progress made.

The author has highlighted potential shortcomings in their ability, highlighting issues such as dealing with people and being quick to shut off when a topic doesn't interest them. Whilst these can be a barrier to some success, being aware of the weaknesses is the first step to be taken in addressing them, and work can be done to become stronger in these areas.

Finally, an awareness of soft skills has been demonstrated from multiple sources, by highlighting the skills required for both academic and professional success allowing for effort to go into improving these soft skills with the aim to put themselves in situations where these skills are needed. Since practice remains one of the most important factors to becoming better at something.

Higher education is more demanding, with self-motivation and organisation being key to success, by planning ahead, creating timetables and being more aware of their personality type

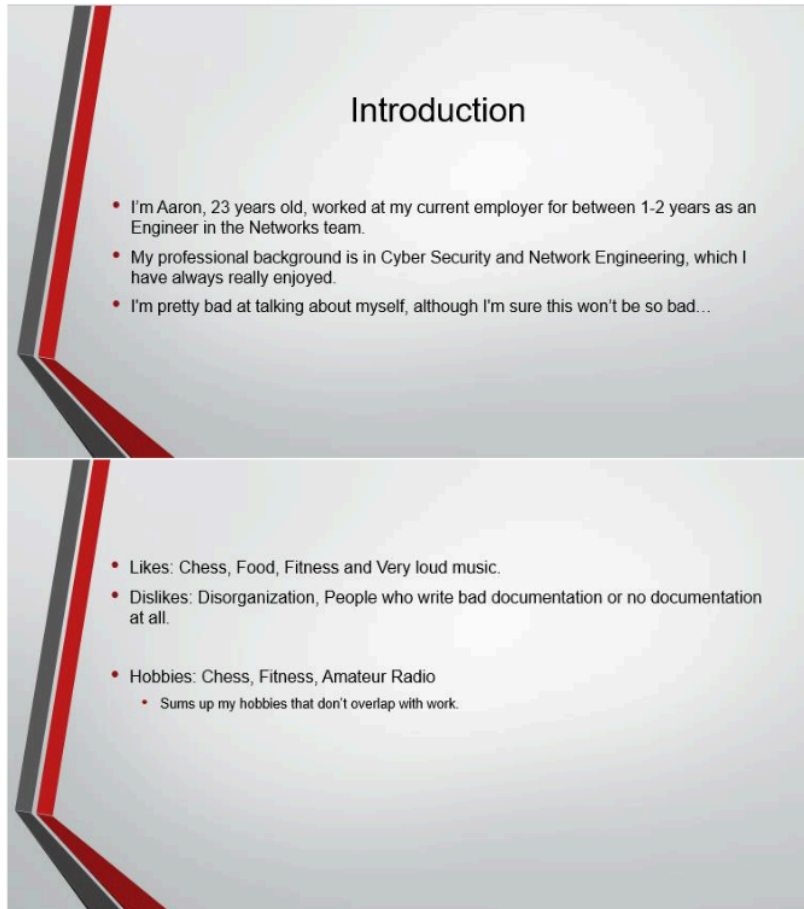
through taking tests, the author can better understand their strengths and weaknesses, using this knowledge to forward their academic success and know where they might struggle before they find themselves in a situation where they may not be so productive or could struggle with stress and other emotional factors.

6.0 References

- [1] O. Schinkton, "Student Skills List - 10 Skills Students Need to Be Successful," 12 Jan 2017. [Online]. Available: <https://www.linkedin.com/business/learning/blog/higher-education/10-skills-all-students-need-to-be-successful>. [Accessed 9 Jan 2025].
- [2] Indeed, "12 student skills that are useful for your studies," Indeed, 2024 July 2024. [Online]. Available: <https://uk.indeed.com/career-advice/career-development/student-skills>. [Accessed 9 Jan 2025].
- [3] UK National Careers Service, "Develop your soft skills," National Careers Service, [Online]. Available: <https://nationalcareers.service.gov.uk/careers-advice/how-to-develop-your-soft-skills>. [Accessed 9 Jan 2025].
- [4] National Careers Service, "Skills assessment," National Careers Service, [Online]. Available: <https://nationalcareers.service.gov.uk/discover-your-skills-and-careers>. [Accessed 9 Jan 2025].
- [5] US Office of Disability Employment Policy, "Soft Skills: The Competitive Edge," US Department of Labor, [Online]. Available: <https://www.dol.gov/agencies/odep/publications/fact-sheets/soft-skills-the-competitive-edge>. [Accessed 9 Jan 2025].
- [6] Fortinet, "CIA Triad," Fortinet, [Online]. Available: <https://www.fortinet.com/uk/resources/cyberglossary/cia-triad>. [Accessed 11 Jan 2025].

7.0 Appendices

Annex A – Screenshots from presentation



S/W

- Strengths:
 - Can focus quite well on subjects I enjoy.
 - I do actually enjoy giving presentations/speaking, but usually about research or a technical topic.
 - I can remember random details and facts, which is useful sometimes
- Weaknesses:
 - Dealing with people
 - Overcritical sometimes, slight perfectionist
 - The opposite of focusing well on some subjects, I can be quite quick to shut off if it's not something that I enjoy...

The future?

- Ideally to finish my degree and earn some other qualifications in the next 4 years.
- This probably isn't the exact subject I see myself building a career in, but I still enjoy it and find it interesting...
- In 10 years I have three main goals:
 - Complete the BEng and go on to do a MSc in Wireless Communications or Cyber Security
 - Achieve a CCIE Enterprise (Cisco Internetwork Expert)
 - Achieve a CCIE Wireless
 - Hopefully if I achieve all of these to move abroad and work for Cisco, Nokia or Broadcom etc.

Annex B – Personality test results

These are the results of the **Fisher Temperament Inventory**. The FTI measures the expression of four temperaments, each of which are presumed to be caused by a specific neurochemical system in the brain. Scores on its four scales range from 0 to 43.

Temperament	Associated neurochemicals	Your score
Curious/Energetic	dopamine, norepinephrine	25/43
Cautious/Social Norm Compliant	serotonin	33/43
Analytical/Tough-minded	testosterone	37/43
Prosocial/Empathetic	estrogen, oxytocin	10/43

Temperament description

Your answer profile matches most strongly to the **Analytical/Tough-minded** temperament. This temperament is dominated by the neurotransmitter testosterone, which promotes confidence, aggression and rule based thinking. People with this temperament are competitive and direct.

Results summary

Your results from the IPIP Big Five Factor Markers are in the table below. The table contains a raw score and also a percentile, what percent of other people who have taken this test that you score higher than.

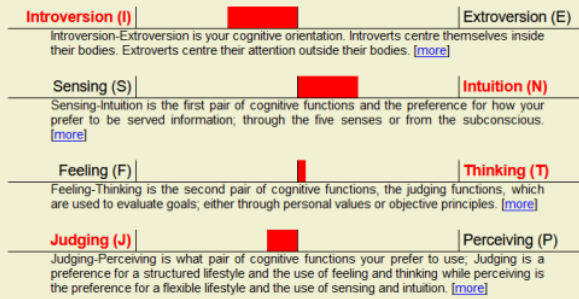
Factor	Factor label	Raw score	Score percentile
I	Extroversion		6
II	Emotional stability		74
III	Agreeableness		9
IV	Conscientiousness		87
V	Intellect/Imagination		65

Big five personality trait scores calculated by openpsychometrics.org

You have completed the personality test.

[Tweet](#)

Jungian/Myers-Briggs Personality Type is based on four preferences, that when combined produce personality type. This page will first cover your scores for each of the preferences then finally give a description for the type that they produce.



When combined, that makes your personality type INTJ. A detailed description of this personality type is below.

People with the INTJ personality type are known for their high level of self-confidence, analytical skills, and strategic thinking. They are deeply independent, preferring to rely on their own intellect and logic rather than follow popular opinion or tradition. INTJs are characterized by their clear vision of the future and a relentless drive to achieve their goals, often displaying a remarkable ability to turn theories into solid plans of action.

INTJs are inherently curious and enjoy delving into complex problems, making them excellent problem-solvers. Their minds are constantly working to generate new ideas and theories, which they approach with skepticism and rationality. They are particularly adept at identifying inefficiencies and developing innovative solutions to systemic issues. This ability makes them excellent in roles that require strategic planning and an analytical approach. Despite their introverted nature, they can be fiercely independent and decisive, trusting their intuition and knowledge to guide them.

[Annex C – Example of a SMART Goal](#)

NOTE To Reader: This was supposed to include 4 goals, however it kept crashing my word and would not format properly for unknown reasons.

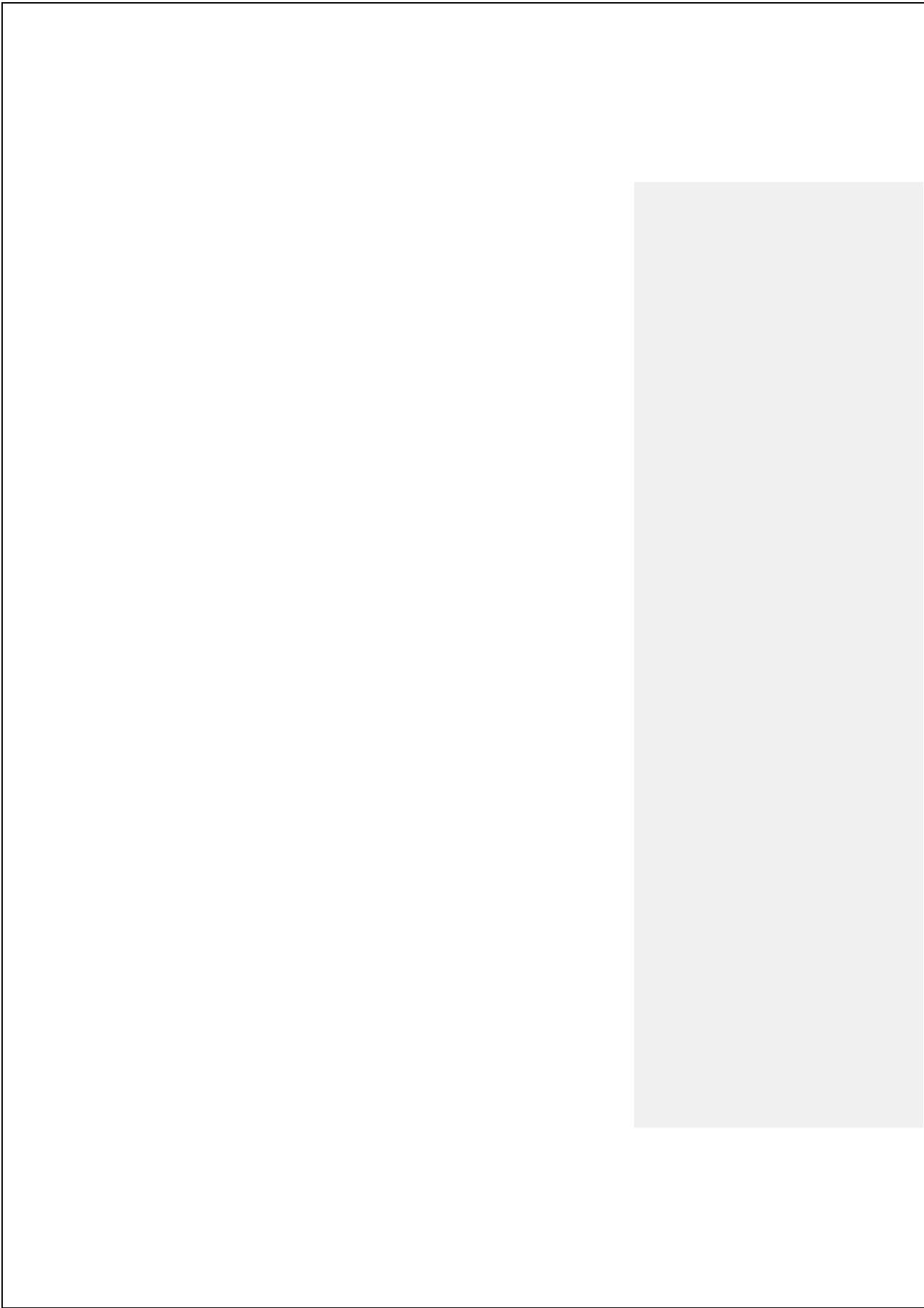
Action Plan

My goal is To reach an 1800 ELO rating online (Up from 1500) and 1500 rating over the board (up from Unrated) in chess in the next year.

Date to finish	How will I measure my success?	
31/12/2025	ELO rating	
Steps to Achieving my Goal		
Description	Time Estimate	Completion date
Persist with regular study of strategic themes, since it remains my weakest point in chess.	Ongoing	
Play regularly online and in ECF rated club leagues.	Ongoing	
Ensure I review any tricky lines in my repertoire on the training software in a timely manner.	Ongoing	
To complete two cycles of the Woodpecker method, improving tactical pattern recognition.	6-8 weeks	
Complete and over study all ~500 variations in Simans endgame course.	2-3 months	
Obstacles that may arise	How I will respond	
Losses along the way, mistakes and blunders in winning positions.	Review and analyse all games that I play and learn from my errors.	
Sheer volume of things to learn/practice.	Prioritise based on my weaknesses (Strategy and positional 1.d4, Nf6 games)	
Helpful Tools	Helpful Resources	
Chessable move trainer	My collection of chess books, opening theory, tactical puzzles and strategic themes	

Annex D – ME+ Time Planner

[illegible]



Ransomware report

Please note: GPT was used to proofread this report, however it did not create any original content. All of the text is derived from the author's original writings.

Also as this is unmarked the author did not complete a disclosure form, but deems that note to be enough.

Contents

1.0 Introduction	14
2.0 Ransomware-as-a-service (RaaS)	14
3.0 Tactics, Techniques and Procedures	15
3.1 Targeted Recruitment	15
3.2 Vulnerabilities	15
3.3 Compromised Accounts	15
3.4 Social Engineering	15
3.5 Previous infections	15
3.6 Third Parties	16
4.0 Real World Examples	17
5.0 Countermeasures	17
5.1 Procedures and Documentation	17
5.2 Backups	17
5.3 Security Training	17
5.4 Network Segmentation	18
5.5 Detection and Response	18
6.0 Conclusion	18
References	19

1.0 Introduction

Ransomware is a variant of computer malware designed to cause significant impact to organizations and individuals through the simultaneous exfiltration and encryption of valuable information. Often run by cybercrime gangs using an affiliate program, the cybercrime gang manufactures the ransomware, while affiliates are responsible for the initial access or compromise of targeted networks. Ransomware can have a high impact on business continuity but remains relatively rare.

Once an affiliate obtains the malware, they deploy it onto a network they have access to. It will then begin moving laterally across the network, spreading to any networked or internetworked machines. Eventually, after a period of time has elapsed, the encryption phase is carried out, along with the optional exfiltration of data.

One key note is that this form of malware is used by both cybercriminals and nation-state supported groups, with different objectives and tactics, techniques, and procedures (TTPs). Both usually aim to obtain money; heavily sanctioned countries may use ransomware as a means to raise funds they would otherwise struggle to acquire.

For the purposes of this report, we will only discuss the cybercriminal side of ransomware, as discussing nation-state attacks and advanced persistent threats is out of scope.

2.0 Ransomware-as-a-service (RaaS)

Ransomware operates as a highly effective business model for criminal gangs. Before delving into the technical details, we will first look at how ransomware seeks to extort victims and then a look at how a RaaS model operates.

Once the malware has been deployed, users are usually greeted by a pop-up informing them of the infection and demanding a ransom paid in cryptocurrency (traditionally Bitcoin (BTC) or Ethereum (ETH), although Monero (XMR) has become the coin of choice for cybercriminals due to its inherent anonymity) in exchange for a decryption key that will restore the files to their original state. A further tactic often used is the threat of selling exfiltrated data, serving as an additional incentive to pay. Known as "double extortion", this tactic comes into play if the organization has an effective backup scheme and is not concerned about data recovery but is worried about the release of sensitive data to the public.

The business model varies from group to group, with notable examples being the REvil and Conti ransomware gangs, who operate a Ransomware-as-a-Service (RaaS) model. These models involve either targeted recruitment of affiliates or the typical approach any company takes when selling a product, such as advertising and comparing to competitors in order to win customers.

Companies often pay these ransoms, more often than not because they would rather keep data breaches quiet due to concerns such as fines from regulatory bodies, reputational damage, etc. It is estimated that around 75% of ransomware attacks go unreported, as reported by the US Cybersecurity and Infrastructure Agency (CISA). [1]

Commented [I1]: Explain the model here

Commented [I2]: Doesn't really explain RaaS, maybe make a flowchart?

3.0 Tactics, Techniques and Procedures

In this section, we discuss some of the TTPs used by RaaS groups to target organizations and the technical methods that have been used in the past or are currently in use by active groups today.

TTPs used for ransomware do not differ much from those for general vulnerabilities; however, there are a few common attack vectors often utilized by groups to gain initial access to a network.

3.1 Targeted Recruitment

As previously discussed, the model of relying purely on affiliates to gain access while the ransomware groups code and sell the malware is common among cybercrime groups. This model can take many forms and may involve targeted recruitment by a ransomware group seeking to attack a particular organization. For example, in 2020, a Russian citizen flew to the US and initiated contact with an Uber employee he had met a year earlier, offering a \$1 million bribe for the employee to either open a malicious email attachment or use an infected USB stick to gain access to Uber's internal network and deliver a piece of ransomware. [2]

3.2 Vulnerabilities

Machines exposed to the internet are open to scanning by cybercriminal actors, whether they already know the address through an internal contact, are able to resolve the address of web servers, or actively search for specific machines or software using a technical search engine such as Shodan [3]. This contributes to an organization's attack surface, where any machines with vulnerabilities accessible from the web present an opportunity for threat actors to gain initial access, particularly if vulnerabilities such as privilege escalation or remote code execution are exploitable.

3.3 Compromised Accounts

Compromised accounts can vary in definition. For this report, we will discuss the approach of password spraying. This technique involves attackers using pairs of credentials (i.e., username and password) that were previously exposed in data breaches. The exact source of these credential pairs is typically the dark web, where many forums and marketplaces offer dumps from data breaches—sometimes for free, but often for the highest bidder, as seen in the case of the now-defunct Raid Forums [4]. Sometimes, these data dumps may even originate from previous ransomware attacks.

By using password spraying and credential pairs, attackers create less noise than a traditional brute-force attack, but it is still considered to fall within the same category. It also generates numerous logs, which system administrators and security personnel can monitor for anomalies.

3.4 Social Engineering

Taking advantage of the weakest link—the human factor—attackers use manipulative techniques to gain information or assist other attack methods, such as phishing. Previously, the author of this report wrote about the concept of con games [5]. This illustrates how attackers exploit human responses to factors such as authority, consensus, scarcity, urgency, familiarity, and trust.

On its own, this is not a technical technique. However, when paired with a scenario where an attacker receives an MFA prompt after finding a valid pair of credentials, it becomes more effective. If the attacker has access to the employee's phone number, they may attempt to manipulate the employee into revealing the MFA code, thereby gaining access.

3.5 Previous infections

Threat actors often do not want to leave a system they have already compromised. Persistence is a key objective in the cybersecurity kill chain. Whether through a direct backdoor in code or

software, or by implanting command and control infrastructure in the target network, an attacker will often maintain a presence even after achieving their objectives, allowing them to return at a later date and strike again. This is why activities such as threat hunting and regular evaluation of network or firewall logs are essential for maintaining a secure network.

3.6 Third Parties

Third parties also represent a key entry point, with many companies and enterprises deploying Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), or Infrastructure-as-a-Service (IaaS). These vendor relationships mean that the vendor will hold important data about their customers. Additionally, in some cases, vendors may have direct links into an enterprise network, such as with services like EDR (Endpoint Detection and Response), where a client is present on enterprise machines and connected to a controller in the cloud. This creates the potential for a compromised service provider to push out malicious code via an update. While this example may not be the most realistic, it can happen to any software supply chain.

4.0 Real World Examples

This section has been left out for purposes of university report and is left in as a template for the author's blog.

Commented [13]: Maybe include a section on emerging trends?

5.0 Countermeasures

Combating ransomware from a blue team perspective remains, like most things in cybersecurity, a difficult task. It requires a multi-disciplinary approach, involving skilled security engineers and analysts who deploy and monitor infrastructure, as well as specialists who design and deliver effective security training to end users. The approach will vary depending on the company, its customers, and the industry in which it operates. However, it is possible to generalize the objectives of cybersecurity personnel into a few key points:

1. Document and understand the environment.
2. Recruit and continuously upskill personnel.
3. Maintain the environment through patches, updates and vulnerability management.
4. Deliver ongoing security training to end users.
5. Conduct penetration testing or adversary emulation exercises.
6. Document lessons learned from incidents and exercises and revisit the first step.

The above list is not exhaustive, but it provides a good starting point. The sections below expand upon both proactive and reactive measures that technical and business teams can take to maintain defences and prepare for a ransomware attack.

5.1 Procedures and Documentation

In relation to the first step, the environment consists of the network architecture, critical assets, and vulnerabilities that already exist within that environment's software, hardware, or firmware. Understanding your attack surface and implementing asset management is a critical step that must not be overlooked. This step is vital for detecting anomalies, prioritizing, and implementing effective security controls.

Building on the above, planning procedures and establishing a Computer Incident Response Team (CIRT) or outsourcing those responsibilities is an important proactive step to ensure that when incidents occur, there is a documented response that is immediate, thorough, and measured.

5.2 Backups

Commented [14]: Potential Over-Reliance on Backups

Ransomware seeks to undermine the availability of organizational and customer data, which, if successful, has a significant impact on operations and can affect the ability to meet agreed-upon Service Level Agreements (SLAs). To combat this threat, regular backups should be performed using appropriate schemes, such as the grandfather-father-son method, and tested to ensure that restoration can be done quickly and that personnel are comfortable with the process.

It is important to note that attackers who compromise a system and maintain a long dwell time may already be present in data backups. This means that when you restore the backup, they can easily redeploy any malware contained within it. For this reason, it's crucial to use additional methods to reduce the dwell time of an attacker and minimize the likelihood of this occurring.

5.3 Security Training

Personnel are a critical part of any organisation, and it is vital to ensure they are aware of common concepts such as phishing, password security, and safe online practices. Providing them with the ability to recognise potentially malicious attempts to obtain information or unknown attachments/software with the purpose of causing harm through ongoing security awareness training is essential.

Often the most significant and insecure attack surface, it is up to security teams to ensure their users are well-educated, confident, and able to scrutinise, act appropriately, and report anything they feel could be malicious.

5.4 Network Segmentation

Network segmentation allows for the separation of different areas of the network, such as placing less critical departments on a different part of the network or implementing a demilitarized zone (DMZ) to separate internet-facing network elements from an organization's internal network. Combined with the assumption that an attacker has already compromised the network (a component of a zero trust model), network segmentation, if implemented correctly, can greatly reduce the impact an attacker can have on critical network elements.

This technique serves to limit the spread of malware and makes it more difficult for an attacker to move around the network during the initial access phase. Ultimately, it requires more effort from the attacker, which presents a greater opportunity for analysts to detect anomalous behaviour early in the attack lifecycle.

5.5 Detection and Response

Reducing the dwell time of an attacker and responding to threats quickly is usually the role of a security analyst. By looking at telemetry received from security tools within the enterprise, it is their responsibility to identify and prioritize threats based on the alerts and information received.

Tools such as Endpoint Detection and Response (EDR) allow for continuous monitoring of endpoints such as laptops, computers, and mobile devices—a step up from traditional signature-based antivirus software [6]. EDR can aggregate logs and provide deeper insight and context into what is happening on a device, allowing security analysts to hunt threats and respond with speed and precision.

6.0 Conclusion

Ransomware remains a significant threat to organizations and, to a lesser extent, individuals. By practicing good cyber hygiene and understanding the threat, the cybercriminals who use ransomware to make money and cause damage to organizations can be defeated. However, it remains a challenging task and requires skilled security teams to effectively fight back.

This report has provided a high-level overview of the world of ransomware, from exploring the business model operated by cybercrime gangs to explaining why ransomware is such an effective business. It also investigates the TTPs of attackers and suggests potential countermeasures to prevent and limit the damage that a ransomware incident could cause to an organization.

As ransomware continues to evolve, security teams must stay up-to-date on current threats and techniques. Understanding the attacker is the first step toward outsmarting and defeating them, thereby protecting an organization and its customers from breaches and business downtime.

Commented [15]: However, it would benefit from more in-depth technical analysis, a discussion of the challenges in implementing security measures, and a more nuanced exploration of emerging trends and ethical considerations.

References

- [1] D. Jones, "Feds remain in the dark as ransomware disclosure lags," Cybersecurity Dive, 25 May 2022. [Online]. Available: <https://www.cybersecuritydive.com/news/senate-ransomware-cisa/624369/>. [Accessed 24 November 2024].
- [2] P. H. O'Neill, "How a \$1 million plot to hack Tesla failed," MIT Technology Review, 28 August 2020. [Online]. Available: <https://www.technologyreview.com/2020/08/28/1007752/how-a-1-million-plot-to-hack-tesla-failed/>. [Accessed 24 November 2024].
- [3] "Shodan: Search engine for the internet of everything," [Online]. Available: <https://www.shodan.io/>.
- [4] S. Bocetta, "Recapping Raid Forums: The Place Where Data Was Sold To The Highest Bidder," Level Blue, 18 Oct 2024. [Online]. Available: <https://levelblue.com/blogs/security-essentials/recapping-raid-forums-the-place-where-data-was-sold-to-the-highest-bidder>. [Accessed 2 Dec 2024].
- [5] A. Bell, "Con Games. How do they do it?," AACYBER, 20 Jun 2022. [Online]. Available: <https://aacyber.uk/2022/06/20/con-games/>. [Accessed 2 Dec 2024].
- [6] Microsoft Security, "What is endpoint detection and response (EDR)?," Microsoft, [Online]. Available: <https://www.microsoft.com/en-us/security/business/security-101/what-is-edr-endpoint-detection-response>. [Accessed 30 December 2024].

Study Skills assignment FINAL Aaron Bell

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

71 /100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

GRADING FORM: GJ_2019

AARON BELL**355****ENGAGEMENT WITH LITERATURE**

Some very relevant sources cited with good implementation of the IEEE format, however even more references could have been included (10-20 were suggested in the brief)

65**KNOWLEDGE AND UNDERSTANDING**

A very competent level of K&U demonstrated.

78**COGNITIVE AND INTELLECTUAL**

Most areas well analysed as opposed to simply presenting data.

75

PRACTICAL APPLICATION



Generally a good level of evidence presented on the use of the various tools etc, however the reason given for not showing an e-portfolio just ends up getting a zero mark for that aspect!

68

TRANSFERABLE SKILLS



An excellent level of grammatical ability.
Generally well laid out and presented, however no TOC included

69