Addressing the Skills Shortage

Gareth Davies, Angela Mison and Peter Eden

University of South Wales, Treforest, UK

Gareth.Davies@southwales.ac.uk

Angela.Mison@southwales.ac.uk

Peter.Eden@southwales.ac.uk

Abstract: Security by design is an up and coming paradigm which seeks to decrease the opportunity for corruption and disruption, and to increase the inherent stability, dependability and resilience of systems. Cyber experts need to be involved in the design phase as Finagle's Law, interpreted for cybersecurity, is 'if it can be hacked, it will – at the worst possible time'. Testing is designed to counter Murphy's Law and reduce resistentialism. Defensive programming, original cybersecurity, carries an overhead, for which there is often no demonstrable return. The priority of the design stage cybersecurity expert is to plan for contingencies and think like a hacker. It is about risk management; understanding this dictates security by design requirements in the knowledge that interconnected systems' security is only as strong as its weakest link. Definition and audit of Service Level Agreements (SLA) are an essential part of cybersecurity, as is the audit of any third party suppliers of componentry of the system under design. Governance and policy definitions, exciting for some, are integral to cybersecurity. Beyond this, the cybersecurity expert must consider system failure. Recent ransomware attacks have demonstrated the necessity for business continuity plans as recovery has still taken time. The Blue Team Field Manual has an impressive list of necessary documentation and actions required in this event, but glosses over the effort required. While the above is rolling maintenance, threat hunting differs. Every vulnerability or threat must be evaluated for consequential impact. Either a passionate interest in psychology or an extremely jaundiced view of the world is a necessary attribute for cybersecurity. Reality is so different from the aspirations of potential pen testers, incident responders, and AI security engineers facing 3 – 5 post-graduation years to proficiency, it is no wonder disillusion results in a shortage of 3.5 million cybersecurity experts.

Keywords: Murphy's Law, Finagle's Law, Resistentialism, Cybersecurity, Career path

1. Introduction

Everyone, everywhere, will have come across Murphy's and Finagle's Laws, and experienced resistentialism. To understand how they relate to cybersecurity requires their definition.

Murphy's Law – *If it can go wrong it will*, although the original, stemming from 1948, is stated as *if there is more than one way to do a job, and one of those ways will result in catastrophe, then somebody will do it that way* (Murphy, 2012). It remains a tenet of defensive design, and translated to the cybersecurity context - *if it can be hacked it will*.

Finagle's Law of Dynamic Negatives – *if it can go wrong it will – at the worst possible time* (techopedia, 2021), is a corollary to Murphy's Law giving recognition to the inevitability of negative outcomes occurring, but which, due to timing, amplify adverse effects.

Resistentialism – *the seemingly spiteful behaviour manifested by inanimate objects where those objects cause problems and exhibit malice to humans* (Jenning, 1948)

Cybersecurity – and now comes the difficulty. There are many definitions, most of which emphasise the technical:

Cybersecurity refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cybersecurity may also be referred to as information technology security. (Digital Guardian, 2021)

It all seems do-able, until you get the definition from people who really know what they are talking about:

Cybersecurity is how individuals and organisations reduce the risk of cyber attack. (National Cybersecurity Centre, 2021)

Cybersecurity has suddenly gone from devices, networks and all things technical, to something amorphous, waffly, and boring. It permeates the entire organisation and culture, where the buck stops with the Board who,

in the UK, are responsible and accountable, potentially personally and financially liable due to inadequate reporting of solvency and risk (Financial Reporting Council, 2016), both of which can arise from cybersecurity failings. The least that can happen in response to a publicly advertised security breach is loss of reputation for the organisation concerned. Where quoted, the market demonstrates loss of confidence, with an immediate reduction in share price,

Although addressing the banking industry, The Financial Conduct Authority (Steward, 2021) Discusses the role of self interest of senior managers and their potential personal liability. Seen from this perspective cybersecurity is not about securing anything, it is about risk management, both personal and organisational, and organisational continuity. When an organisation suffers a cyber-attack, one has to ask why cybersecurity is held responsible for a consequential organisational failure in addition to the technical failure. If a house falls down, is it the electrician's fault? When the skills shortage is discussed, it is not certain exactly what skill is in short supply and whether some skills could and should be available from non-technical areas.

It has been shown that risk management by itself cannot provide a complete solution yet low-level technical graduates are being asked to make decisions about risk mitigation and business continuity, often when cybersecurity has failed. Those graduates thought their jobs would be exciting, like gaming, fighting black hats and fixing battle damage. There is a mismatch of expectation, responsibility, and accountability.

Technical cybersecurity is a post hoc system development add on - on par with extended testing, proving the presence of errors, never their absence. It is necessitated by the inevitable inadequacy of the system design phase, failure of the resultant implementation, lack of business planning and lack of top-management understanding of the consequences of business decisions in an interconnected world. Incident response is the reaction to failure of cybersecurity. In reality, it can lead to organisational upheaval.

2. The real purpose of cybersecurity

Cybersecurity addresses, in part, technical systems. Its broader definition (*ibid*) comes from viewing systems in their context. Only truly failed systems exist in a vacuum - implemented, but not installed. Systems are developed to support something. In the manner of an inverted triangle, what they support is some type of purposeful organisation, thus cybersecurity's goal is to enable continuity of the organisation dependent on that system.

The analogy of the inverted triangle is useful to define purposes and consequences. An upstanding inverted triangle is inherently unstable. The organisation can be represented by the whole while the technical systems are at the base point. Tamper with the base, and the whole or part may topple, taking with it continuity of operation. The real purpose of cybersecurity is to prevent that toppling and ensure continuity if the triangle does topple. Incident response is equivalent to FEMA after the earthquake, concerned with clean up and rebuilding, with prevention of repetition in mind.

3. Cybersecurity in the organisation

3.1 Specialist selection – team portfolios, diversity, and human resources

There is a requirement for detailed definitions of roles within an organisation. These normally encompass the necessary skill sets (NICCS, 2021). Forward looking organisations recognise that any successful team requires a portfolio of skills and mind sets (Patterson, 2018). When examining a vacancy, it is necessary to identify both the skills that are missing, the mind set which will enhance team performance, and then to describe that unicorn. A passionate interest in psychology or an extremely jaundiced view of the world may be a necessary attribute together with disillusion caused by Murphy's law.

Formulaic selection can miss the greatest talents and closest matches to an organisation's actual needs which are often based on less obvious factors and which, unexpectedly, may be found in-house in a different field. Unfortunately, outsourcing and automated selection techniques can be the same as asking the wrong question, where the answer does not matter, and consequently, a limited talent pool is presented. Currently, it is reported that 99% of Fortune 500 companies use some form of applicant tracking systems (Qu, 2019)

Cybersecurity resourcing supports the argument for a Chief Neurodiversity Officer (Levell, 2017). It maybe that the inherent mind set of an applicant is more important than skills which can be learnt, extended or covered by

others, and more deterministic of suitability of a candidate and the ultimate career path. Is a detail oriented person required, or is it someone whose mind is buzzing with half-baked ideas? A good recruiter knows who, in his team, has these traits, and whether more of the same, or different traits are needed.

3.2 Security by design – architects, designers and risk managers

Security by design seeks to reduce the opportunity for corruption/disruption of a system and to increase its inherent stability, dependability and resilience. There is a need for the involvement of cyber experts in the design phase. Murphy's Law of computing systems failing at introduction should resonate. Given a choice of options in a requirements specification, the developer is not necessarily the best person to determine the direction of the organisation through an apparently logical, but ultimately disastrous choice. It must be pointed out that cybersecurity experts are exempt from neither Murphy's nor Finagle's Law.

The priority of the developer is getting the system to fulfil the requirements. Defensive programming, the well understood original cybersecurity, can carry a large overhead for which there is often no demonstrable return, and which, if developed without consideration of psychological consequences, can increase any inherent resistentialism. Good user interfaces result from extensive research..

The role of the cybersecurity expert at this stage is to identify what the system can be made to do, define contingencies, the 'what if', scenarios, being aware of the threat landscape and thinking like a hacker. It behoves the cybersecurity expert to believe the worst of the world and to dictate the requirements for extended defensive programming in order to defend against the foreseeable.

Worse than this, the cybersecurity expert needs to understand the context in which the system operates - an increasingly interconnected world with complex supply chains. The security of an interconnected system is only as strong as its weakest link, and organisational hubris may lead to the assumption that this is elsewhere. An internal weakness may expose the organisation to, at least, compensation claims from interconnected parties, while a suspected weakness in an interconnected party may suggest intrusive investigation.

Risk management in system development requires an unusual skill set dealing with evaluation of consequences and mitigation decisions. The cybersecurity version of this includes the answer to 'if this failed, what would we need to do to keep operating?'. That answer incorporates continuity which should be added to any process documentation – not obviously a cybersecurity role, but in the broad definition, yes, it is.

Cybersecurity adds to cost and is subject to criticism. The difficulty is one faced by intelligence Services: how to appreciate and value the effort of protecting against something that does not happen, but which event is a possibility? If the event did happen, it could be organisationally existential.

3.3 Murphy's and Finagle's Laws and resistentialism – testers

It is a sad fact that development projects are constrained. There are only three factors to consider in a project: time, resources, and money. Some would argue quality, but that is taken as a given here. Where a project is running late, testing is usually the economic sacrifice. Testing proves the presence of errors, never their absence. In pure system testing, it is the place to find errors and iron out the bugs and irritations attributable to Murphy's Law and resistentialism.

An additional, separate test suite is required to meet the requirements of security by design. Whether this is a formalised test suite based on scenarios, and/or letting the technical experts try a little pen testing is cultural. The testing must take place in context, i.e. its interconnected state, and this would be the ideal time for ethical pen testing of partners.

3.4 Supply chain and interconnected parties – procurement, quality, legal, risk, auditors

The position is simple; if your organisation can hack into interconnected systems, so can someone else, which opens your organisation to potentially unconsidered risk. Of course, having the ability to do this depends on your position in the food chain, the leverage you can exert, and whether your ethics, contracts, or Service Level Agreements (SLA) with others permit arrogation of their systems.

Discussion of SLA with interconnected parties has not been seen as the preserve of the cybersecurity expert. Audit of compliance with the terms of the SLA is an essential part of cybersecurity, as it will be structured to ensure those terms. Beware: compliance does not equate to performance!

Resilience, dependability and integrity requirements may require the continuous monitoring or audit of any third party suppliers of componentry or systems under consideration. Where there is a less than cooperative party, there is a higher risk and arrogation may be necessary to ensure cybersecurity and potential continuity of operation. In a third party supplier relationship, the ongoing nature of their business, continuing longevity, quality and rights to fundamental materials and documentation in case of their cessation of trading or existence may be elements for inclusion in contracts or SLA. This inclusion protects the maintenance and continuing operation of said systems in the short term.

The skill sets for definition and audit of such elements may not be the preserve of the cybersecurity expert, but any organisation of note will have a legal, financial, procurement departments capable of cooperating to include the requisite cybersecurity requirements. Collaborative working of this nature increases the cybersecurity expertise and culture in these disparate areas and increases the organisational awareness of the cybersecurity expert. This exchange and extension of knowledge is beneficial both personally and organisationally.

3.5 Policy and Governance – lawyers, psychologists, human resources, change managers

Policy and governance changes are often the result of an event and designed to prevent repetition. For most, policy and governance definitions are not exciting parts of the cybersecurity remit, but remain essential. To technical people, change management has hitherto been associated with endless documentation arising from the change to one or more lines of coding. Furthermore, the cybersecurity expert must consider system failure, at which point, all hell breaks loose, but which hell must somehow be constrained into processes and procedures, and communicated within the organisation.

The banking industry is addressing conduct and culture. Interestingly, (Group of 30, 2018) states:

Conduct is not just about purposeful misbehaviour, but also unintended consequences from decisions and/or lack of skills and knowledge.

Policy and governance actually dictate the way personnel should behave and the way the enforcement regime. Understood slightly differently, this equates to the culture of the organisation. From this perspective, any change, to a policy or its governance, represents a cultural or behavioural change, usually not attainable by diktat, but more by persuasion and education. Habitually there is resistance to change, thus change management has a skill set in its own right, addressing the needs of personnel and smoothing transitions wherever possible.

An example of a novel cybersecurity policy which may encounter resistance is the termination of use of personal devices or personal internet usage. There are very good cybersecurity reasons for these particular policies, but given the attachment people have to their devices, or web surfing, they are policies which may meet with resistance and need careful management, education and reinforcement to achieve a more cyber secure workplace. This example demonstrates that edicts, emanating from the basement, where the cybersecurity 'geeks' hang out and are detached from reality, can have profound effects on organisational behaviour, culture and even induce organisational churn. Having said that, it highlights the 'us and them' mentality that may exist.

This is a relatively obvious example. It should be borne in mind that any policy and/or governance changes affect everyone in the organisation and thus the important consideration is how to achieve their adoption without disruption. The interaction of change managers and cybersecurity experts may be beneficial, increasing the empathetic skills of the cybersecurity personnel, and leading to informal communication with relevant personnel preceding the release of a new or changed policy – sometimes wording and tone matter, as does an understanding that the language used must be appropriate for its audience.

3.6 NOCs, SOCs – technical experts

Attacks do not need to be direct, they can be consequential, from an attack on a third party attempting to corrupt or manipulate something entirely different, somewhere else. Going back to the system design and development phase, what can the system be made to do, and if you were a hacker, how might that be

monetised? Every identified vulnerability or threat must be evaluated in this light. As with all things cyber, risk management cannot stop at the borders of the organisation.

The NOCs and SOCs are similar to continuous testing and monitoring for those Murphy's and Finagle's Laws events, the one's for which there is no contingency. There is an unfounded belief in project and programme management that where there is a contingency plan for an event, that event will not happen, but some other event will. This adequately describes the behaviour of IDS and IPS. Some of these events may be induced through internal system errors or introduced by malefactors or inattentive interconnected partners so the cybersecurity personnel have to adapt to detecting and exercising their expertise in a high pressure environment, recognising that no matter what they do, they will be held to blame for any organisational failure. They need to be protected from unrealistic demands and harrying regarding any progress and this can be provided by the cybersecurity incident response team (CSIRT) processes and procedures allied with continuity plans.

4. Incident Response – the organisation

4.1 Incident Response – technical experts

Cybersecurity experts are not exempt from Murphy's Law. It is always assumed that cybersecurity will fail, otherwise there would be no pre-ordained CSIRT or procedures. While something is floating around the network, it cannot do too much damage, but if it becomes active in any node, there is a problem. Incident response is the answer to the failure of cybersecurity.

Often the malefactor's intent does not manifest to defenders until there is an observable event which is detected in the system or an organisational functional area by means of unexpected behaviour of the system. Periods for detection can be protracted due to user expectation of resistentialism, or belief that an update has taken place which has altered the behaviour of the system. 'The system is slow today' can hide a multitude of problems. Reporting is problematic.

Bearing in mind the speed of the internet data transmission is of the order of 178 terabits per second (Nield, 2020), and a round trip between Europe and the USA takes approximately 70 milliseconds (Brown, 2013), it is useful to consider a domino race analogy, applied to the topology, understand where potential break points might be defined and the near impossibility of stopping anything in the time available once it is past the IDS. It is impossible to fix anything unless you have an idea of what it is, i.e. what it might be doing and where it might be. Anyone with experience of mission critical systems will recognise that any bug fix can only take place when the bug has been found, no matter what the SLA says.

4.2 Incident Response – technical experts, lawyers and public relations

The incident response functions are activated on the recognised failure of the cybersecurity system and process which has a consequential impact on continuity. Post event, it takes on a forensic aspect, followed by a clean-up and revisions to policies and procedures. It can never be assumed that all traces of an event have been eradicated.

If the organisation is outward facing or there are interconnected parties, legal and communication issues arise. There are a number of public facing organisations who have dealt with this over the years, and the continuing difficulty is in the determination of timing of normal service resumption, the parties who should be notified, any lasting damage to systems, and the effect on continuity. There is a current assumption that any public notification of website technical issues or reduction of system functionality due to updates are the result of a hack. Whether this is true, it represents a major inconvenience to any users and may be detrimental to the organisation.

4.3 Business continuity – the Board, finance, legal, and essential organisation functions

Recently, the necessity for business continuity plans has been demonstrated as a result of ransomware, but it has still taken time to overcome disruptions, and to recover. The Blue Team Field Manual (White & Clark, 2017) has an impressive list of necessary documentation and actions required in the event of cybersecurity failure. It does not indicate the effort required to complete the documentation, but the knowledge and expertise involved in their production indicates that it is extensive. For an organisation to produce such documentation is a major project.

The continuity plan that is contained within the documentation may deal with the complete failure of organisational systems eg ransomware, when continuity may mean reverting to manual processing. Off-site, disconnected back-up systems may be instantiated but, depending on back-up frequency, there may be a loss of data in the interim. There may be plans to isolate the organisation from authorised interconnected third parties when the necessary continuity plan may mean manual operation of parts of the business, for example supply chain, or alternative bulk data exchange mechanisms. How the continuity plan is implemented, depends on the definition of the mission critical parts of the organisation function and non-corruption of associated critical network paths.

Continuity management (CM), an organisational responsibility, implies that continuity plans are in place. When cybersecurity fails, the situation frequently degenerates to crisis management, not at all the same thing. There is a marked difference in the results achievable when an ordered rather than chaotic approach is taken as noted by the Civil Contingencies Act Enhancement Programme (Cabinet Office, 2012). At no time should organisational continuity be the sole responsibility of cybersecurity.

4.4 Maintenance – the organisation

Maintenance or changes, recommended or mandatory, are usually the result of some event and incident response pursuant to a post event audit, similar to a forensic analysis of processes and procedures. Updating the relevant systems and/or paperwork is undertaken in an attempt to prevent a repetition of that event which caused a cybersecurity failure and to improve the response to such a failure. Its primary purpose should never be apportioning blame.

Maintaining documentation relating to policies, governance, contracts, SLA, processes, procedures, key staffing lists etc can be a much hated task to the cybersecurity expert. Any chore which is much hated is unlikely to be done well, so revelling in such a detail oriented task is a characteristic that should be sought.

As can be seen from the roles exemplified in the organisation it may be that the task of maintaining certain cybersecurity elements is best delegated to whence ever the source of the original. This requires negotiation with other departmental heads as it requires allocation of their resource. They departmental heads will know if maintenance is possible within the time constraints of an individual, or if some reshuffling of work is necessary.

Part of maintenance is an element of succession planning or ensuring redundant resource to enable cover. There is a need to know who is doing what, and what happens if a key person leaves or succumbs to some illness. This becomes particularly relevant if legacy systems are involved, as one financial institution found to its cost. Part of maintenance is securing the continuity of knowledge and process. The organisation is not a collection of silos; it is a collection of interdependent interconnected systems, whether those systems are manual or technology based.

5. Intelligence

Most commercially available cybersecurity systems are reactive. Threat hunting is an intelligence based activity. There are many threats, but to carry out an informed risk assessment determining which ones warrant preventive investment, requires knowledge of the systems and its interconnections. A technical person who understands what organisational systems can be made to do and who can think like a hacker is unlikely to be on staff, but there is always hope. Technology and malefactor tactics develop rapidly, and it is no longer necessary for an attacker to have technical skill as the required software can be commissioned or acquired, ready for use, on the dark web. It is worth noting that a criminal mindset in which access is assumed, leads to a serendipitous calculation of how to monetise that access. A purposeful attack is redolent of a structured organisation, while the opposite is true for an opportunistic attack.

Intelligence is perhaps best suited to someone with a vacuum cleaner mind, who absorbs knowledge from anywhere and everywhere, analyses it internally, and makes connections. This mindset is epitomised in Six Days of the Condor (Grady, 1975), and in the 'Machine' in the television series Person of Interest (Person of Interest, 2011). It is the proactive branch of cybersecurity, and as such could also be useful in the defensive system design stage.

There are times when it useful to have social networking skills through which malefactors identified with specific skill sets can be tracked and their contacts monitored to prevent a crime as a service incident.

6. Monopoly of big tech and cybersecurity

In the move to the Cloud, organisations are outsourcing aspects of their cybersecurity, and are likely to have no access to policies and procedures or system workings of the Cloud Service Provider (CSP). This presents problems where one or more co-tenants may have the possibility to attack the underlying systems. Due to dependence and lack of alternatives, organisations may be forced to accept the assurances given by CSP.

A further concern is that public and private organisations may become the training grounds for cybersecurity resources. They will be unable to compete with the rewards offered by big tech when proficient cybersecurity experts look for their next post.

7. Conclusion

Selection to organisations is often made on the basis of outgoing personality, the ability to interact favourably in interview. It is common knowledge that all things being equal, the person that is liked more, is the one chosen. Sometimes this may not be the right choice as the best technical cyber experts may be somewhere on the autistic spectrum (Payne, et al., 2019) or operating in a different functional area of the organisation.

With the global cybersecurity workforce shortage equating to 3.5 million, it has to be asked if this is for the purely technical aspects or whether cybersecurity is assuming responsibility for all organisational failures. University courses are churning out potential pen testers, incident responders and AI security engineers, all supremely technical, but who will never be sufficient in numbers to provide all the skills required to fill the breach. The reality of cybersecurity is very different from their aspirations and expectations, and career progression not always obvious.

It is recognised that the term 'cybersecurity' may be off-putting to the non-technical. As usual, language and tone matter. Couching the consequences in relevant terms, enables the posing of questions to start discussions and enumerate solutions. Within University courses and organisational table top exercises, the questions – 'How would you do this without a computer?' or 'How essential are you to the organisation and why?', would lead to personal investment in the solutions and perhaps change the cybersecurity culture.

The inverted triangle that is the organisation need not rest solely on its tip, but could have metaphorical re-bar running throughout. Between the technical level and the Board are functions where inherent cybersecurity abilities and proclivities may be found and utilised. Education of the organisational functionaries should include elements of cybersecurity, but in audience appropriate language: the implications of consequential breach, social engineering, organisational continuity, and cyber safe understanding. In this way, cybersecurity culture will permeate the organisation, spread the load to where the continuity expertise resides, and reduce the pressing demand for the missing 3.5 million.

Cybersecurity should have a proactive service aspect, where personnel can come for advice or guidance. It is not sufficient for it to be just the reactive defence force. The answer to the skills shortage may be dependent on the definition of cybersecurity and continual acceptance of responsibility for organisational failings.

References

- Brown, G., 2013. Fourteenth Annual Sommerville Lecture: The wrong questions about cyberspace. *Military Law Review*, Volume 217, pp. 214-233.
- Cabinet Office, 2012. *Chapter 6 Business Continuity Management*. [Online] Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61029/Chapter-6-Business-Continuity-Management_amends_04042012.pdf [Accessed 16 September 2021].
- Digital Guardian, 2021. *A Definition of Cyber Security*. [Online] Available at: <https://digitalguardian.com/blog/what-cyber-security> [Accessed 9 September 2021].
- Financial Reporting Council, 2016. *Guidance on the Going Concern Basis of Accounting and Reporting on Solvency and Liquidity Risks*. [Online] Available at: <https://www.frc.org.uk/getattachment/62ae3969-fe26-4def-8d25-e2acd821e7b1/Guidance-on-the-Going-Concern-REVISED-WEB-READY-2016.pdf> [Accessed 16 September 2021].
- Grady, J., 1975. *Six days of the Condor*. London: Hodder & Stoughton General Division. Group of 30, 2018. *Banking Conduct and Culture: A permanent mindset change*. [Online] Available at: https://group30.org/images/uploads/publications/aaG30_Culture2018.pdf [Accessed 16 September 2021].
- Jennings, P., 1948. Report on Resistentialism. *The spectator*, 23 April.

- Levell, J., 2017. *Rise of the Chief Neurodiversity Officer*. [Online] Available at: <https://www.neurocyber.uk/post/rise-of-the-chief-neurodiversity-officer> [Accessed 13 September 2021].
- Murphy, C. E., 2012. *Murphy's Laws Origin*. [Online] Available at: <https://militaryhumor.net/murphys-laws-origin/> [Accessed 9 September 2021].
- National Cyber Security Centre, 2021. *What is cyber security?*. [Online] Available at: <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security> [Accessed 9 September 2021].
- NICCS, 2021. *Home Page*. [Online] Available at: <https://niccs.cisa.gov/> [Accessed 15 September 2021].
- Nield, D., 2020. *Researchers Just set a new record for the fastest internet speed ever*. [Online] Available at: <https://www.sciencealert.com/researchers-just-set-a-new-record-for-the-fastest-internet-speed-ever-recorded> [Accessed 26 June 2021].
- NIST, 2017. *Federal Cybersecurity Coding Structure*. [Online] Available at: <https://www.nist.gov/document/federalcybersecuritycodingstructure-v20-10-18-17docx> [Accessed 15 September 2021].
- Office of the Under Secretary of Defense for Acquisition and Sustainment, 2021. *Security Maturity Model Certification*. [Online] Available at: https://www.acq.osd.mil/cmmc/docs/CMMModelExcel_V1.02_20200318.xlsx [Accessed 15 September 2021].
- Patterson, G., 2018. *Fighting Cybercrime with Neuro Diversity*. [Online] Available at: <https://www.project-syndicate.org/commentary/neuro-diversity-cybersecurity-autism-asperger-by-gavin-patterson-2018-01?barrier=accesspaylog> [Accessed 13 September 2021].
- Payne, K.-L. et al., 2019. Is there a relationship between cyber-dependent crime, autistic-like traits and autism?. *Journal of Autism and Developmental Disorders*, Volume 49, pp. 4159-4169.
- Person of Interest*. 2011. [Film] United States of America: Kilter Films; Bad Robot Productions, Warner Brothers Television;.
- Qu, L., 2019. *99% of Fortune 500 Companies use Applicant Tracking Systems*. [Online] Available at: <https://www.jobscan.co/blog/99-percent-fortune-500-ats/> [Accessed 17 September 2021].
- Steward, M., 2021. *Compliance, Culture and Evolving Regulatory Expectations*. [Online] Available at: <https://www.fca.org.uk/news/speeches/compliance-culture-and-evolving-regulatory-expectations-mark-steward> [Accessed 16 September 2021].
- techopedia, 2021. *Finagle's Law*. [Online] Available at: <https://images.techopedia.com/definition/19342/finagles-law> [Accessed 9 September 2021].
- White, A. & Clark, B., 2017. *Blue Team Field Manual*. version 1.2 ed. Scotts Valley(California): CreateSpace Independent Publishing Platform.