Strategic Cyber Environment Management with Zero Trust and Cyber Counterintelligence

TT Bodström

University of Jyväskylä
Faculty of Information Technology
Jyväskylä, Finland
E-mail: tero.t.bodstrom@student.jyu.fi

Abstract: *Organisations need to improve their information security practices, given the volume of successful cyberattacks and crimes. To enhance security in an organisation, information security must be considered a business issue, instead of a technical problem. Hence, organisations must change the security protocol from reactive action to proactive operation; must develop information security strategies that support the business; should implement better controls, systems, and services; and must create a process to proactively gather information about the possible threats and adversaries. This study proposes a novel method for combining a zero-trust strategy with cyber counterintelligence to gain the required security level and situational awareness to encounter modern threats.*

Keywords: *Information Security Strategy, Zero Trust, Cyber Counterintelligence*

Introduction

A major problem today is in the number of cyberattacks against organisations, which can be seen in the growing number of data breaches and other successful attacks. These attacks include advanced persistent threat (APT) attacks, fraud, ransomware, insider threats, and other cyber domain incidents (Sigholm & Bang 2013). Due to the COVID-19 pandemic (INTERPOL 2020), and the associated increasing number of remote work, attacks have risen significantly. This has caused organisations' networks to be even more complex than earlier, uncontrolled, and more vulnerable. EY Global Information Security Survey 2020 (Lovejoy 2020) found that 65% of organisations are reactive regarding cyberattacks; that is, they respond only after the incident has occurred. This is a clear indication of the tendency to protect existing systems by adding security tools to fulfil checklist compliance instead of building security into systems.

In many organisations, the information security (IS) strategy can be considered a necessary document that must be written due to information security standard requirements, instead of being a useful document to steer information security in a manner that supports the business. A global information security survey affirms that only 8% of organisations have an information security function that supports business needs (EY 2018). The results of a workshop questionnaire in 2018 revealed that only approximately 30% of workshop attendees had fully achieved a written information security strategy (Bates & Young 2018). Even though these percentages are low, it is not clear how well they can be generalised to all organisations. Nevertheless, if the earlier numbers, 8% and 30%, are even close to reality, the situation is worrying. The questionnaire used by Bates and Young (2018) did not reveal whether the IS strategy was implemented to support the business strategy. It is obvious that business strategy demands the support of IS strategy and not the other way around; otherwise, information security is implemented for its own sake. Further, the information security strategy should be evaluated regularly and compared to the business strategy to verify that they are aligned.

Previous research (Ahmad, Maynard & Park 2014), literature review, and discussions with eight security managers pointed out that most organisations use strategies only to keep information technology available and to comply with IS standards. It is of concern that business risks are ignored by most of the security managers, and for deploying strategies, systematic development was not used; instead, strategies were deployed on an ad-hoc basis. The results also showed that in all cases, security strategy was driven from bottom to up, not from top to bottom in organisation hierarchy (Ahmad, Maynard & Park 2014). Further, strategies were technology driven, which led to situations where all threats were treated or solved with technical solutions, instead of resolving the human dimensions via training, education, security awareness, or by changing organisational culture towards security.

These issues require more novel and sophisticated measures to implement more control of networks and security to systems along with the methods that are proactively providing early warnings of threats. The mentioned countermeasures also need to be applied when ad hoc remote connections are used. Hence, the usage of offensive cyber counterintelligence (CCI) is justified, as James Olson, former CIA director, wrote:“CI that is passive and defensive will fail. We cannot hunker down in defensive mode and wait for things to happen” (Olson 2002).

This conceptual paper presents how the zero-trust network, together with cyber counterintelligence, implements a robust method for solving the mentioned issues and proposes a strategic steering process for maintaining IS strategy updated. This study addresses the issue from a strategic point of view, but tactical, operational, and technical details are not covered. Moreover, in this study, risks are considered from the threat point of view, although the author acknowledges that risk can also be an opportunity.

This qualitative research study is based on a literature review of selected papers and an analysis of the various presented methods. In the first phase, the papers were selected based on keywords and abstracts. Then, the selected articles were studied, and a final set of references was selected to obtain background knowledge about the related earlier studies and commonly known issues.

Previous Studies

Effective counterintelligence protects and supports business strategy and intelligence. Cyber counterintelligence (CCI) is considered a subset of counterintelligence, and besides protecting intelligence, it creates inside information about the adversaries. It also measures deception and disinformation to support an organisation in achieving its goals (PC Duvenage & Solms 2014).

To overcome the challenges and complexity of cyber counterintelligence, that are involved in out-thinking and outwitting of actual and potential adversaries, a three-dimensional matrix tool was proposed. The matrix presents the following premises for the optimal development of offensive and defensive tools: passive-defensive, active-defensive, active-offensive, and passive-offensive, while considering strategic, operational, tactical/technical as a third dimension (PC Duvenage & Solms 2014; Duvenage, Jaquire, & von Solms 2019). These proposed premises are also considered in this study from a strategic level; however, active-offensive tools are considered only for intelligence gathering purposes, not cyber weapons points of view.

Adjustments were suggested to the three-dimensional matrix model, originally proposed in 2014, by dividing the four premises into five dimensions to achieve a multi-discipline maturity model. Each dimension is divided into three sub-dimensions: strategic, operational, tactical/technical. All sub-dimensions are then divided into six different areas of compliance: structures, people, processes, technologies, legal and policies, and training and skills development. However, this list is not exhaustive; thus, it can be adapted to organisations' requirements. The purpose was to create a cyber counterintelligence maturity model, which can be easily adopted for different types of organisations, where the focus is in line with capabilities, strategy, and realities (Jaquire & von Solms 2017).

The importance of an accurately developed and executed CCI process was emphasised to proactively weaken sophisticated cyber threats. However, the CCI process must be separate from cybersecurity processes, which are mostly activities driven by compliance, where technical aspects dominate. International standards that provide cybersecurity processes for all types of entities are insufficient (Duvenage, Solms & Corregedor 2015). The international standards have been criticised for being too generic or universal; thus, they do not consider the organisation's specific structures or security requirements (Siponen & Willison 2009). Further, CCI is missing academic research, and it is poorly understood by public and commercial disciplines. While it is important to conduct research, the basic principles must be right from the beginning. The intelligence cycle does not support the counterintelligence process as it was developed for the positive intelligence process. For these reasons, a theoretical model with a single continuous process, which has two non-linear and overlapping sub-processes, offensive and defensive, was presented (Duvenage, Solms & Corregedor 2015).

Two different machine learning models based on natural language processing (NLP) for cyber threat intelligence (CTI) were tested to generate new information from publicly available data. The research results showed that NLP has potential as a tool for providing useful information for cyber threat intelligence (Voutilainen & Kari 2020). The major difficulties in a cyber domain are: i) knowing when one has been attacked, ii) what indeed happened, ii) what the consequences are, and iv) who the attackers are. Another challenge is to identify the correct data from the huge amount of data that is available and to understand whether the data is useful or not. To solve these issues and identify information leakages in a network, a technical concept was presented (Sigholm & Bang 2013). The concept relies on a centralis (Duvenage, Solms & Corregedor 2015) document fingerprint database and CCI sensors that analyse document fingerprints passing through a network. Further, with a trusted partner network, sensor networks can be expanded to identify whether the documents have been leaked (Sigholm & Bang 2013).

While cybersecurity processes are commonly based on standards and best practices to achieve protection against cyberattacks, they do not take into account how the adversaries act. So, strategies are considered from the defender's mindset, which leaves a big gap for understanding how the controls should be set up and prioritised. For this reason, there is a need for a regular steering process that 1) compares IS strategy with a current business strategy to verify the accuracy, 2) performs counterintelligence analysis to understand adversaries' modus operandi (MO) and tactics, techniques, and procedures (TTPs), and 3) reviews and adjusts incident reports for controls, if earlier selected controls are not correctly set up.

Zero Trust

A great concern is that victim networks are breached a lot earlier than the attack is detected, with the average detection time being 206 days (Oosthoek & Doerr 2020), which is a long time period. This happens also in controlled networks; a successful attacker might need only one vulnerability to penetrate the network or system, while a defender needs to defend all possible vulnerabilities. This creates a high asymmetry between attacker and defender, and the overall security level is as low as the weakest point. Even though the protection of networks and systems cannot reach 100% security, organisations should protect them better by avoiding poor or no protection. One possible solution is the zero-trust framework, which provides a strategic-level guide for how protection is implemented.

Zero trust, which was presented in 2010 (Kindervag 2010), is a holistic method for network and service protection, with the strategy "Never trust, always verify". The fundamental idea is that all networks, known and unknown, are treated as hostile, assuming that the aggressor is already inside the network. Therefore, by controlling and limiting access through network micro segmentation—users, user groups, devices, software, time, geolocation, and so forth—it is possible to set up a highly controlled network. Zero trust also emphasises the importance of monitoring, logging, and auditing networks and devices that are connected to it, as well as all user activity. The physical devices must be protected (passive-defensive [Duvenage, Jaquire, & von Solms 2019]) against tempering and unauthorised device implementation, such as network devices that can intercept traffic and USB drives that can install malware, spyware, and so forth to compromise a cyber environment.

The zero-trust strategy was implemented to test the platform with firewall, automated, and centralised logging tools, and dynamic firewall access control lists (ACL), which adjusted rules for rejecting or dropping traffic when attacks were detected. The model also utilised dynamic trust levels based on the authorised connections. Detection tests showed low latency detection and ACL modification times, which suggests that automated detection is faster than human action. Zero trust is also a working solution when implemented correctly. However, attack tests were executed only with distributed denial of service (DDoS) attacks (Eidle *et al.* 2017), and another attack type of detection requires verification and possibly additional functionalities for detection.

By controlling and limiting access through network micro segmentation, users, user groups, devices, software, time, geolocation, and so forth, can achieve a good overall picture of what is happening inside the network using zero trust. It offers incident reports that are used for adjusting controls, and case reports show incorrect control placement and prioritising. However, the method itself does not offer an outside view, particularly regarding who is threatening.

Inside view: Insider threats

It is a fact that the number of attacks caused by insider threats is increasing (Hu, Li & Fu 2015; Eidle *et al*. 2017). Charney (2019) studied the psychology of insider threats in intelligence communities, how insiders are successful, and described the major reasons for success as follows: “The real challenge: how to protect our secrets when we don’t know what secrets have been given away to our enemies by unidentified insider spies, working in the shadows for years on end with no outward drama.” One can assume that the analysis is correct in other public and private organisations. Usually organisations become aware of the insider threat after someone from the recruiting side reveals the breach (Charney 2019).

Even though it is extremely difficult to predict who will be an insider threat, zero trust offers countermeasures against this type of behaviour. For example, a user can try to access documents where he or she does not have access rights, install unaccepted software on the device, execute unauthorised network scans, and so on. All previous actions cause alerts in cases where the threshold is set up correctly. Too low a threshold is causing a lot of false alerts, and too high is causing the opposite issue, where nothing is considered as malicious. Thus, when the zero-trust strategy is implemented and technical solutions are configured correctly, the possibility of a successful insider threat attack is lower, as their activity causes weak signals of abnormality. However, these measures and countermeasures do not address outsider threats, more specifically, who is threatening, and which are their TTPs. Additional information for weak signals can be gathered with passive network sensors and devices.

Passive sensors are devices that are placed in network environments’ strategic places and act as decoys (passive-offensive, active-defence [Duvenage & Solms 2014; Duvenage, Jaquire & von Solms 2019]) to monitor unexpected behaviour. The idea is that, in a normal situation, they should receive a minimum amount of traffic, if at all. These sensors are awaiting connection attempts, which can be unusual port knocking or network scans from an unusual source, for example. The mentioned attempts must be interpreted as weak indicators and should be monitored when they occur. The behaviour can be caused by an insider with no malicious intention, an insider with malicious intention, or an ongoing network attack.

From a technical point of view, there are multiple ways to implement these sensors. Multiple studies have identified network attacks with different methods with machine learning and its subset, deep learning (Sigholm & Bang 2013; Bodström & Hämäläinen 2019). There are also known methods for setting up decoys for networks, such as honeypots, which act as dummy servers in a network. However, the honeypots have been in the market for a while, and advanced attacks can identify them based on their signatures. However, it is a good practice to set up some honeypots to network, as they report signals of unusual behaviour. More than one incident yields a more confident result of the detected behaviour.

This can be a procedure for forcing attacks to cause more signals to network. When detecting a honeypot, the attack usually stops trying to break in and continues to the next possible target. Besides honeypots, commonly known vulnerable servers with meaningless information can be set up (passive-offensive [Duvenage & Solms 2014; Duvenage, Jaquire & von Solms 2019]) or even malware to interfere with the attack. The vulnerable servers are interesting targets for an attack, diverting the attention of the attack on them. However, there is no guarantee that the attack will go first to a honeypot; the attack can start directly from the vulnerable server. Indeed, the network topology needs to be implemented in such a manner that these decoys are not located in an important network segment; instead, they run in a shared micro segment where other networks have full access.

Other passive sensors are intrusion detection system (IDS) network devices and software, which inspect network packets from the data flow. Their purpose is only to identify anomalies and unusual behaviour, instead of dropping packets, which is the firewall and intrusion prevention system (IPS) task. These sensors can have different mechanisms for detection, such as signatures based on earlier known attacks. Due to the heavy development of hardware and computing power, many anomaly detection solutions also utilise machine and deep learning techniques.

Information from passive sensors can be combined for a richer overall network picture. The information from different sensors can be used to make cross-checking for alerts, which is viewed as a capability to reduce the number of false alarms. However, passive sensors do not disclose anything about existing server and service vulnerabilities in a network. For identifying those, a vulnerability assessment is required. The purpose of vulnerability assessment is to verify which systems in an organisation have vulnerabilities. This helps to gain a better overall understanding of the cyber environment and its security level. Found vulnerabilities are prioritised and patched. While executing the assessment, the report revealed by the IS regarding network scanners and via error messages should be verified. Cyber criminals use the same techniques while executing reconnaissance in networks, and by comparing results, it is possible to find detailed attack vectors from the common vulnerability and exploit (CVE) library or for zero-day vulnerabilities. Hiding this information is not a security measure; instead, it is a simple countermeasure that will buy more time to detect anomalies in systems and networks. While cyber criminals cannot access applications information and their version numbers, they will need to perform different actions to penetrate the systems. This will cause detectable signals, even weak, if systems and logs are monitored for anomalies.

The passive sensors and vulnerability assessment together produce an overall understanding of existing risk areas in the network and systems, that is, how those are protected, where the controls are located, as well as what type of data is passing via the network in normal situations. By actively monitoring incidents and verifying them, one can generate inside reports for checking if the controls are set up correctly and for executing countermeasures as well. The monitoring will also produce reports on which information is used in the strategic steering process.

Cyber counterintelligence: Outside view

CCI, as described earlier, is a sub-branch of counterintelligence, while CTI, besides risk intelligence, is a sub-branch of CCI. Even though their purposes are the same, both intelligence types use different types of gathering data to obtain better knowledge about the adversaries. In what follows, the line between the intelligence types are drawn.

The purpose of CTI is to gather information about adversaries (active-defensive, active-offensive [PC Duvenage and Solms 2014; P Duvenage, Jaquire, & von Solms 2019]) from networks, instead of trying to find exploitations for vulnerable systems. There are multiple free and commercial services that provide general information related to common threats (Oosthoek & Doerr 2020). This type of information is useful until a certain level. The issue is that, when asked what the real threat is, the answer is no longer obvious. Hence, the threat intelligence has gone deeper in a networked world; that is, besides the public network, data also needs to be obtained from the dark web.

The results of NLP usage in CTI showed that the approach is useful for gathering more data (Voutilainen & Kari 2020). The public can obtain data from open threat exchange (OTX) sites, such as AlienVault (https://otx.alienvault.com/). These sites offer more detailed information about the attacks and related indicators of compromise (IoCs). Another important source of information is the dark web. With the Onion Router (TOR) client, hacker forums and cybercrime marketplaces can be accessed to acquire more data and information related to an organisation that needs to be protected. By combining these three different source types, the information is enriched, as it considers the technical data from OTX as well as the data from cyber criminals from the dark web.

However, even though the benefits of CTI usage are undeniable, CTI itself is still an immature process, delivering broken products. The major issues are 1) the lack of methodology—even conference speakers refer to well-known methods, such as Structured Analytic Techniques (SAT), but they cannot point to how it is utilised, 2) CTI uses data inputs to create alerts rather than analytical hypothesis, 3) information is shared but rarely used, 4) low quality data, for example biased Indicators of Compromise (IoC) raw data, indicates only possible compromises, not verified compromises, 5) CTI sells a huge amount of data, which needs to be filtered and analysed before usage and 6) CTI data feeds are biased towards sensors that gather data (Oosthoek & Doerr 2020).

With risk intelligence, the organisation gathers and processes information about the operational area to face and handle challenges and to make sense of related attributes. The purpose of the mentioned information is to help to make strategic decisions (Stouder & Gallagher 2015); thus, counterintelligence is a process that also requires a strategy (Stouder & Gallagher 2013). Therefore, besides CTI information, there is a need to understand cyber criminality in an operational area. The cyber criminals in different countries and continents have different MOs; therefore, it is not possible to assume that, for example, the same type of information security controls or training are suitable for every location. It is possible to create general basic-level standards, training, and guides for information security; however, it is necessary to tailor everything else to suit the operational area. Hence, the risk intelligence (active-defensive, active-offensive [Duvenage & Solms 2014; Duvenage, Jaquire, & von Solms 2019]) helps operators understand how local cyber criminals are acting.

Major risks in the operational area are found in the governments' and the international organisations' publicly available data. Besides the crime rate and types, these statistics offer data from other types of risks, such as political situations, natural disasters, and public infrastructure reliability. Private companies can also conduct risk assessments for countries, which may be a useful data source. When this information is used together, overall risks can be estimated in the operational area and countermeasures can be considered.

Even though many governments and international organisations are offering cybercrime-related data, these statistics are somewhat unreliable, as victims of cybercrimes do not readily report crimes to police. Victim organisations treat these issues mostly privately when it is possible. Nonetheless, this information will present at least a cybercrime trend in the operational area, even if the confidentiality level for statistics is questionable. The main purpose for counterintelligence gathering and analysis is to obtain knowledge about the adversaries, their MO and TTPs. The counterintelligence will be used in the strategic steering process to predict future cyber threat trends, for example, in one year’s time, and to redefine controls against newly arisen threats. The accuracy of the analysis is evaluated regularly to understand the organisation’s mindset—that is, how much really was understood. The decision makers will be aware of the necessity of counterintelligence.

Support for strategic decision making

Based on the methods reviewed, Five Ws and How (5 WH: Who, What, When, Where, Why, and How) questions offer a better understanding of the adversaries. **Table 1** presents an example.

Who?	is threatening us?
When	do they operate; is there a timewise pattern?
Where	do they operate, cyber space or physical space or both?
Why	do they attack (motive)?
How	do they attack (MO and TTPs)?
What	does this mean to organisation and systems protection

Table 1: 5WH questions

These questions and their answers will facilitate the selection of countermeasures and the type of, when, and where those must be implemented. Without the knowledge of what 5 WH offers, significant amounts of resources may end up being used to incorrectly prioritise to secure or secure completely wrong objects, which causes vulnerabilities. Once an organisation has implemented an information security strategy that supports a business using a robust tool, such as Sherwood Applied Business Security Architecture (SABSA, https://sabsa.org/), it is important to follow up on the selected strategy and controls. The follow up process can be implemented with the earlier presented methods.

One tool for the process is the intelligence circle although it has been criticised (Duvenage, Solms, & Corregedor 2015); the intelligence circle is executed as a continuous process. The data sources presented in the section on inside and outside views are used as data sources for the loop. Due to the type of data received, it is possible to generate reports on what has happened as well as a strategic analysis for possible outcomes shortly. Possible controls that support an information security strategy can be defined with the strategic analysis. The analysis will reveal the possible attackers and their TTPs, and it will help define how and where to set the focus for protection. On the other hand, as one also knows the weaknesses and vulnerabilities in the environment that are to be protected, more monitoring focus can be targeted. The zero-trust strategy offers guidance for controls.

With all information, it is possible to verify, for example, annually, whether the selected controls are correct compared to threats and risks. That is, one can make an analysis for the next year; however, there is a monthly follow-up based on the situation reports. If the selected controls are not in line with the actual situation, they can be adjusted for consistency with the information security strategy. The information security strategy also needs an annual follow up. It is possible that the business strategy has changed during the year and is no longer aligned with the information security strategy. The annual check meeting should also include strategic analysis for the following year and feedback from the previous year, particularly regarding how correct the last analysis was and what needed to be realigned.

The entire proposed strategic steering process is described in **Figure 1**.

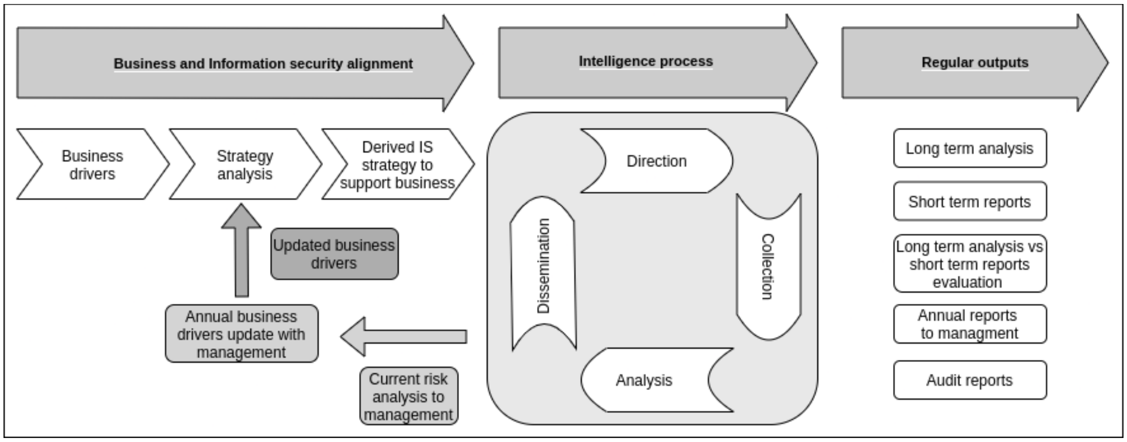
Business and Information security alignment
Intelligence process
Regular outputs
Business drivers
Strategy analysis
Derived IS strategy to support business
Updated business drivers
Annual business drivers update with management
Current risk analysis to management
Direction
Collection
Analysis
Dissemination
Long term analysis
Short term reports
Long term analysis vs short term reports evaluation
Annual reports to managment
Audit reports

Figure 1: Strategic information security steering process

Current Issues

Based on the presented relevant information, the following issues need insights to achieve higher-level IS and to more effectively protect organisations' valuable assets.

Organisations must stop thinking of IS as only a technical issue that can only be resolved with technical solutions. The problems are organisation-wide; thus, they must be solved so. This includes training and educating personnel correctly with tailored programmes, not by arranging an annual general training day to achieve standard compliance. Further, organisation-wide cooperation with all risk management sections is needed to accomplish better knowledge about the risks towards the organisation, which at least consists of information technology, financial, human resources, and legal sections.

Statistics show that, in most organisations, IS strategy exists only for standard compliance, and it does not support business strategy at all. Organisations need to acknowledge that the primary function of IS is to ensure that the business continues in all possible situations, even with limited resources. Thus, planning an IS strategy must be invested enough so that it supports business goals. Given that, in many organisations, business goals are changing over time, the need for regular IS strategy evaluation is essential. Otherwise, organisations may have decade-old IS strategies that share no commonalities with current business strategies and goals.

Another known issue is that organisations do not focus enough on network, system, and protection, as revealed by statistics related to successful attacks. A great concern regarding this issue is that organisations are seeking standard compliance; thus, the mentality is biased to standards. That is, organisations expect that when standard compliance is achieved, everything is secure. Standards must be used only as a framework; all outcomes must be tailored, and the protection level must be thought of by the information that is processed in systems. In many countries, information processing is defined by laws and regulations that define the minimum protection level.

Zero trust is a recommended approach for controlled networks and systems, where trust needs to be earned, and it is not given automatically. This will reduce the possibility of successful commonly known attacks, as the attack vectors are better controlled. This will give security personnel more time to seek weak signals that are related to earlier unknown attacks. However, to understand the attackers' TTPs and MOs, a counterintelligence process is also required. However, instead of just gathering adversary-related data, the counterintelligence process also needs a systematic analysis to be useful for decision making. When counterintelligence analyses are added to vulnerability assessment, the understanding of threats against the network and system will increase, as will the overall picture.

Conclusion

The paper presented a conceptual method for improving organisations' information and cyber security by combining a zero-trust strategy and cyber counterintelligence. It is obvious that implementation requires resources; however, improvements are inevitable in the near future. COVID-19 and its impact on the global economy are forcing societies work remotely even more, which increases the need for new digital services and tools. Although cybersecurity is not improving at the same rate, the attack surface for cyber criminals keeps widening. Due to the widening surface, the asymmetry between attackers and defenders increases, as the attacker needs only one penetrable access point, and the defender needs to protect all possible access points.

The zero-trust strategy has been available for a while, and it has been implemented successfully. However, security vendors sell their products as zero trust products, which is misleading, as the term was originally intended to be a strategy. Nonetheless, organisations are recommended to implement zero trust, and they can choose tools freely for technical set up. The National Security Agency (NSA) released a paper entitled "Embracing a Zero Trust Security Model" in February 2021, in which it highly recommends the use of zero trust (US NSA 2021).

As many cyber counterintelligence research publications that were presented in these papers argued, CCI is not yet in a mature state; thus, it requires more research and possibly an academic discipline to achieve a higher maturity state and to be fully accepted. Nevertheless, it is a valid tool for seeking a better understanding of an organisation's cyber environment in an operational area. Improvements need to be made, as the open access days for networks, systems, and services are over; otherwise, there will be a major disaster caused by a cyberattack targeted at critical infrastructure services. In the worst-case scenario, this will lead to a loss of lives.

References

Ahmad, A, Maynard, SB & Park, S 2014, 'Information security strategies: Towards an organizational multi-strategy perspective', *Journal of Intelligent Manufacturing*, vol. 25, no. 2, Springer, Berlin/Heidelberg, German, pp. 357-70.

Bates, C & Young, J 2018, 'Crafting an information security program strategy', viewed 12 May 2021, <https://er.educause.edu/blogs/2018/5/crafting-an-information-security-program-strategy>.

Bodström, T & Hämäläinen, T 2019, 'A novel deep learning stack for apt detection', *Applied Sciences*, vol. 9, no. 6, p. 1055.

Charney, DL 2019, ‘Three part series of white papers on insider threat, counterintelligence and counterespionage’, viewed 12 May 2021, <https://noir4usa.org/complete-white-paper-parts-1-2-3/>.

Duvenage, P, Jaquire, V & von Solms, V 2019, ‘A cyber counterintelligence matrix for outsmarting your adversaries’, *ECCWS 2019 18th European Conference on Cyber Warfare and Security*, vol. 187, Academic Conferences Publishing Limited.

—, von Solms, S & Corregedor M 2015, ‘The cyber counterintelligence process: A conceptual overview and theoretical proposition’, *Proceedings of the 14th European Conference on Cyber Warfare and Security, ECCWS 2015*, pp. 42-51.

Duvenage, PC & von Solms S 2014, ‘Cyber counterintelligence: Back to the future’, *Journal of Information Warfare*, vol. 13, no. 4, p. 42-56.

Eidle, D, Ni, SY, DeCusatis, C & Sager, A 2017, ‘Autonomic security for zero trust networks’, *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 288-93.

EY 2018, ‘Is cybersecurity about more than protection?’ viewed 12 May 2021, <https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf>.

Hu, P, Li, H & Fu, H 2015, ‘Dynamic defense strategy against advanced persistent threat with insiders’, *2015 IEEE Conference on Computer Communications (Infocom)*, pp. 747-55.

INTERPOL 2020, ‘INTERPOL report shows alarming rate of cyberattacks during Covid-19’, viewed 12 May 2021, <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>.

Jaquire, V & von Solms, S 2017, ‘Developing a cyber counterintelligence maturity model for developing countries’, *2017 Ist-Africa Week Conference (Ist-Africa)*, pp. 1-8.

Kindervag, J 2010, ‘Build security into your network’s DNA: The zero trust network architecture’, *Forrester Research Inc*, pp. 1-26.

Lovejoy, K 2020, ‘How to manage cyber risk with a security by design approach’, viewed 12 May 2021, <https://www.ey.com/en_gl/consulting/how-to-manage-cyber-risk-with-a-security-by-design-approach/>.

Olson, JM 2002, ‘The ten commandments of counterintelligence’, *American Intelligence Journal*, pp. 21-26.

Oosthoek, K & Doerr, C 2020, ‘Cyber threat intelligence: A product without a process?’, *International Journal of Intelligence and CounterIntelligence*, pp. 1-16.

Sigholm, J & Bang, M 2013, ‘Towards offensive cyber counterintelligence: Adopting a target-centric view on advanced persistent threats’, *2013 European Intelligence and Security Informatics Conference*, pp. 166-71.

Siponen, M & Willison, R 2009, ‘Information security management standards: Problems and solutions’, *Information & Management*, vol. 46, no. 5, pp. 267-70.

Stouder, MD & Gallagher, S 2013, ‘Crafting operational counterintelligence strategy: A guide for managers’, *International Journal of Intelligence and Counter Intelligence*, vol. 26, no. 3, pp. 583-96.

Stouder, MD & Gallagher, S 2015, ‘Counterintelligence outreach: Building a strategic capability’, *International Journal of Intelligence and Counter Intelligence*, vol. 28, no. 1, pp. 143-55.

US National Security Agency (NSA) 2021, ‘Embracing a zero trust security model’, viewed 12 May 2021, <https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF>.

Voutilainen, J & Kari, M 2020, ‘Strategic cyber threat intelligence: Building the situational picture with emerging technologies’, *European Conference on Cyber Warfare and Security*, 545-XIX.