Computers & Security 133 (2023) 103412

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Zero trust cybersecurity: Critical success factors and A maturity assessment framework

William Yeoh [a,b,1], Marina Liu [a,c,1,*], Malcolm Shore [a], Frank Jiang [a,c,2]

[a] Deakin University, Centre for Cyber Resilience and Trust (CREST), Geelong, Victoria, Australia
[b] Department of Information Systems and Business Analytics, Deakin University, Geelong, Victoria, Australia
[c] School of Information Technology, Deakin University, Geelong, Victoria, Australia

ARTICLE INFO

Keywords:
Zero trust
Critical success factors
Maturity assessment
Delphi method
Cybersecurity

ABSTRACT

Zero trust cybersecurity is beginning to replace traditional perimeter-based security strategies and is being adopted by organizations across a wide range of industries. However, the implementation of zero trust is a complex undertaking, different from traditional perimeter-based security, and requires a fresh approach in terms of its management. As such, a clear set of critical success factors (CSFs) will help organizations to better plan, assess, and manage their zero trust cybersecurity. In response, we investigated the CSFs for implementing zero trust cybersecurity by conducting a three-round Delphi study to obtain the consensus from a panel of 12 cybersecurity experts. We built a multi-dimensional CSFs framework that comprises eight dimensions, namely identity, endpoint, application and workload, data, network, infrastructure, visibility and analytics, and automation and orchestration. Based on the CSFs, we developed a maturity assessment framework enabling organizations to evaluate their zero trust maturity. This paper contributes to a theoretical understanding of how to deploy zero trust from multiple dimensions and offers a viable guidance framework for organizations from a practical perspective. This paper is useful for organizational stakeholders who are in the process of planning, reviewing, or implementing zero trust cybersecurity.

1. Introduction

Recently zero trust has become the top security priority across industries (Golden et al., 2021). Zero trust is a cybersecurity strategy that shifts from a location-centric to a more data-centric approach for better security controls between users, systems, data and assets that may change over time (CISA, 2021). National Institute of Standards and Technology (2020) defines zero trust as a security model and a coordinated cybersecurity and system management strategy acknowledging that threats exist both inside and outside network boundaries. Zero trust suggests organizations should not trust anything inside or outside their perimeters and instead must verify anything and everything before granting access (Kerman et al., 2020). Zero trust offers numerous benefits, such as streamlined security stack, reduced operational overhead, more efficient and flexible onboarding of employees and vendors (Golden et al., 2021).

According to a survey conducted by Microsoft Security (2021), almost all security professionals believe zero trust cybersecurity is pivotal to their organization's success due to strengthened overall security posture and improved user experience. Over the past few years, COVID-19 has accelerated the shift to a hybrid workplace, which has also driven increased adoption of the zero trust (Jakkal, 2021). Zero trust promises to protect data, even when employees access them offsite on their personal devices. Moreover, in view of the anticipated growth of 5 G, cloud computing, artificial intelligence and IoT that results in more data, connected nodes, and expanded attack surfaces, zero trust cybersecurity is even more critical to the cloud- and the mobile-centric world of today's organizations.

Zero trust differs significantly from traditional perimeter-focused security that automatically trusts internal users, it considers the organizational IT network as untrusted to the same degree as the Internet (Campbell, 2020). Zero trust represents a philosophical shift in how security is managed (Golden et al., 2021). The implementation of zero trust is a complex undertaking, involving multiple dimensions.

* Corresponding authors.
E-mail address: liumengyin@deakin.edu.au (M. Liu).
[1] These authors are co-first authors with equal contribution.
[2] Co-corresponding author.

https://doi.org/10.1016/j.cose.2023.103412
Received 14 June 2023; Received in revised form 6 July 2023; Accepted 26 July 2023
Available online 27 July 2023

Table 1
Benefits of Implementing Zero Trust.

Benefit	Source
Enable the modern workplace and digital business transformation by reducing friction and providing secure and flexible access	(Cunningham et al., 2019) (Deloitte, 2021)
Reduce security costs sustainably as IT complexity is minimized	(Cunningham et al., 2019) (Deloitte, 2021) (Adahman et al., 2022)
Prevent malware propagation and lateral movement due to the creation of micro perimeters and more granular network rules	(Bennett et al., 2017) (Cunningham et al., 2019)
Mitigate the damage of data breaches with more visibility into the network	(Cunningham et al., 2019) (Adahman et al., 2022)
Enhance data awareness and insight because zero trust supports data privacy initiatives and it requires an accurate inventory and classification of sensitive data	(Cunningham et al., 2019)
Narrow the scope of corporate compliance initiatives owing to network segmentation	(Cunningham et al., 2019)

However, security leaders and professionals have little strategic guidance where to start implementing it, or they are concerned about the shift in the principles of strategy and architecture required by zero trust (Turner et al., 2021). Boards need to know what knowledge and competencies are necessary to translate knowledge into action (Bobbert and Scheerder, 2020). Hence proper guidance for implementation of zero trust cybersecurity is important.

Yet the extant literature indicates little academic research on the critical success factors (CSFs) and maturity aspect of zero trust cybersecurity. The existing traditional security CSFs are not applicable to the contemporary zero trust cybersecurity (Yeoh et al., 2021). Accordingly, this paper aims to identify the CSFs for implementing zero trust to bridge the research gap that exists between academic researchers and practitioners that enables organizations to better strategize, plan, assess, and manage their zero trust cybersecurity. We used the Delphi method to identify CSFs for implementing zero trust by conducting three rounds of opinion gathering and reaching a consensus with a panel of cybersecurity experts. Drawing on the findings of CSFs, we further developed an operationalizable maturity assessment framework enabling organizations to systematically evaluate their zero trust cybersecurity maturity.

In the next section, we outline the background prior to presenting the research methodology in Section 3. Section 4 presents the CSF findings. Section 5 introduces a comprehensive zero trust maturity assessment framework designed for assessing an organization's zero trust maturity level. In Section 6, the implications for theory and practice and future research are highlighted, followed by the conclusion in Section 7.

2. Background

2.1. Zero trust cybersecurity

The term "zero trust" was popularized by Kindervag in 2010. The main concept behind zero trust is "never trust, always verify" which means that devices or users should not be trusted by default (Golden et al., 2021; Kerman et al., 2020). From the early stages of IT infrastructure, organizations have utilized firewalls as a tool to secure their intranets. As the variety of mobile devices has proliferated and the use of cloud-based services continues to increase, more attack vectors have surfaced, and perimeter security has become increasingly difficult to enforce. At one time most organizations thought of the intranet as a secure place to expose enterprise applications, but now it seems clear that this is problematic.

The perimeter no longer represents just the physical location of the organization, and the inside of the perimeter is no longer seen as a secure environment for corporate devices and applications and personal electronic devices, making the drawbacks of the traditional model of enforcing perimeter security increasingly apparent. Once the perimeter is successfully compromised by an illegal party, they can easily access the organization's privileged intranet (Ward and Beyer, 2014). Therefore, enterprises rethink the traditional network security perimeter and view the intranet as being as risky as the public network, and then deploy network security measures on that premise. In response to the vanishing perimeter, a zero trust strategy has been proposed that focuses on protecting resources rather than the network perimeter, while network location is no longer considered a major component of the resource security posture (Kerman et al., 2020). Zero trust has advantages over traditional cybersecurity strategies (Buck et al., 2021), as outlined in Table 1.

2.2. Zero trust dimension

As summarized in Table 2, several industry players, i.e., Forrester, Netskope, Microsoft, Cybersecurity and Infrastructure Security Agency (CISA) and American Council for Technology-Industry Advisory Council (ACT-IAC) put forward their respective zero trust models and corresponding dimensions. However, their models are not based on rigorous and systematic research, nor there is data or evidence to support the models. Nonetheless, these works serve as a foundation for further study into the CSFs for implementing zero trust.

Drawing on these practitioners' literature, we build a comprehensive CSF framework for zero trust implementation. Fig. 1 illustrates our overarching multi-dimensional CSF framework that comprises all critical dimensions: identities, endpoint, application and workload, data, networks, infrastructure, visibility and analytics, automation and orchestration. Each dimension also includes general details about the governance (CISA, 2021). Each dimension comprises a number of CSFs that is measurable for its maturity level on a scale of 0 to 5 with 5 as the highest level.

3. Research methodology

A Delphi approach was used in this study. This method achieves expert consensus and avoids situations where a single expert leads to bias (Okoli and Pawlowski, 2004), while anonymity encourages creativity amongst participants. As the exploration of zero trust is still in its infancy, there is a need for cutting-edge and worthwhile insights from pioneering experts with extensive experience and influence in industry

Table 2
Matrix Table of Zero Trust Dimensions.

Dimension Organization	Identity/ People	Data	Network	Endpoint/ Device	Application	Workload	Infrastructure	Visibility & Analytics	Automation & Orchestration
Forrester	X	X	X	X		X		X	X
Netskope	X	X	X	X	X			X	X
Microsoft	X	X	X	X	X		X		
CISA	X	X	X	X	X	X		X	X
ACT-IAC	X		X	X	X			X	X
This paper	X	X	X	X	X	X	X	X	X

Fig. 1. High-Level CSF Framework Across 8 Dimensions.

Table 3
Expert Profile.

Expert	Position	Industry
1	Cyber security and risk director	Higher education
2	Chief information security officer	Information Technology
3	Chief cybersecurity advisor	Information Technology
4	Chief information security officer	Insurance
5	Head of cyber strategy and architecture	Insurance
6	IT and information security manager	Retail
7	Chief information security officer	Insurance
8	Head of information security	Retail
9	Digital security and assurance manager	Insurance
10	Cyber security operations manager	Higher education
11	Managing Director	Information Management
12	Head of Cyber Security	Consumer Services

to guide zero trust implementation. Experts are individuals who have an "institutionalized authority to construct reality" (Meuser and Nagel, 2009). Accordingly, experts in this study consist of individuals who are chief information security officers (CISOs) or equivalent who oversee the cybersecurity of the organization (Bogner and Menz, 2009). According to Egfjord and Sund (2020), the recommended panel size for a Delphi study is between 10 and 15 participants. Thus, we chose a median value of 12. We adopted the snowball sampling (or chain-referral sampling) method to identify experts for this research (Creswell and Creswell, 2018). The process started with background research on speakers from leading cybersecurity conferences, followed by a review of their LinkedIn profiles. It continued thereafter with their referrals until we reached 12 experts. The selection criteria we applied were: 1) working as a CISO or equivalent individual responsible for overseeing the organization's cybersecurity; 2) possessing substantial experience (more than 10 years) in the cybersecurity field, including direct involvement in the guidance or implementation of zero trust strategies; 3) gaining industry recognition, for example, giving presentations on zero trust at cybersecurity conferences, or authoring reputable publications about zero trust. To get broader perspectives, we specifically selected experts from different industries, including insurance, retail, IT service, consultancy, home appliance supplier, university, and government agency. All experts of this study are experienced security professionals. The annual revenue for the respective experts' organization is at least USD$1 billion. Table 3 depicts the expert's profile.

Based on an extensive literature review, open-ended interview questions were designed. The first round of expert opinion collection was conducted through semi-structured interviews. It allows the interviews to focus on a particular topic while giving the interviewees room for autonomy to explore other valuable ideas related to the subject that may emerge from their interviews (Adeoye-Olatunde and Olenik, 2021). Given the COVID-19 pandemic, online interviews with cybersecurity practitioners were held at scheduled times and ranged from 50 min to 70 min. All interview sessions were recorded and then transcribed. All transcripts are sent to the experts to check their accuracy. Following Braun and Clarke (2019)'s approach, the thematic analysis method was applied to analyse the qualitative data collected from the semi-structured interviews. A spreadsheet was used to facilitate the data analysis and coding process. The categorized themes and their subcategories form an initial list of candidate CSFs.

In the second round, the list generated in the first round was distributed to the individual experts by email. A 5-point Likert scale (1 being completely not critical and 5 being extremely critical) was used to rate the significance of the candidate CSFs (Yeoh and Koronios, 2010). According to Hasson et al. (2000), central tendencies and dispersion levels should be calculated to reflect the information collected. Therefore, we calculated the mean, median, mode, and standard deviation of the data collected in the second round. We also modified the existing list based on the feedback gathered from the experts in this round.

In the third round, experts repeated the steps of the second round to reassess the critical success factors for which there was no consensus in the second round. Only critical success factors with a standard deviation of 1.0 or less and a mean of 3.5 or higher were included in the final list to ensure that the experts reached a consensus on the final list of CSFs. The results of the second and third rounds are available at shorturl.at/cpyLR or in Supplementary Material 1. Finally, a total of 43 CSFs in 8 dimensions were confirmed and validated by the expert panel. The details of the CSFs are discussed below.

4. Critical success factors

In view of the large set of CSFs, this section presents the key findings regarding CSFs for implementing zero trust in organizations. Appendix A presents the list of 43 CSFs within their respective dimensions. The 8 critical dimensions are identity, endpoint, application and workload, data, network, infrastructure, visibility and analytics, and automation and orchestration. The discussion of the key findings is presented by dimension as follows.

4.1. Identities dimension

Identities are defined as the common dominator across networks,

endpoints, and applications, such as people, services, or IoT devices. When an identity attempts to access a resource, the organization needs to verify that the identity's access is compatible, following the principles of least privilege access (Microsoft, 2021b). Each identity needs to be assured that it has access to the resources within its privileges at the time it is allowed. The policy engine ultimately decides whether an identity is granted access, which is a core element of zero trust.

Perform multifactor authentication. All experts agreed that to authenticate a user's identity, multifactor authentication (MFA) should be used. Multifactor authentication protects the applications by asking users to verify their identity with a second source of validation before access is permitted, such as a phone or a token. One interviewee stated, *"This meant that we need to do a lot more when it comes to identity, things like multifactor authentication, things like contextual authorization, where we consider the time of the day and the geolocation of where authentication is coming from."*

This view was supported by another expert, *"I think from an identity perspective in terms of the controls that you implement around securing the identity, for me, without a doubt, multifactor authentication is probably number one."*

Implement single sign-on (Ferretti et al., 2021). To better facilitate MFA (Sciarretta et al., 2020), the expert panel advocated to implement single sign-on (SSO). SSO not only improves security by eliminating the need to maintain numerous credentials for the same person, but it also improves the user experience by reducing the number of sign-in prompts. One expert summed up that the importance of bundling SSO and MFA: *"This is one of the ways actually having a single sign-on in place allowed us to roll out multifactor authentication quickly. If we don't have a single sign-on, this means that we need to fit the multifactor authentication technology into every single application. While having a single sign-on that sits in front of all the applications that we are using means that we only need to fit multifactor authentication to the single sign-on option. And then basically this opens the gate to more granular control about safety specific applications. But it makes the implementation of multifactor authentication, which is a very important control in establishing a better identity protection capability."* Thus, SSO and MFA should be prioritised and implemented at the same time to achieve zero trust.

4.2. Endpoints / devices dimension

Devices refer to various hardware assets that access data on the Internet, such as smartphones, IoT devices, laptops, bring your own device (BYOD), partner-managed devices, and cloud-hosted servers. Their diversity provides a huge surface area for illicit cyber actors to attack. Organisations should inventory devices (Adahman et al., 2022) and ensure a baseline of device security protection and visibility of the devices themselves (CISA, 2021).

Register devices with identity providers. To monitor security and risk across multiple endpoints used by anyone, the experts believed that visibility in all devices and access points that may be accessing your resources is critical. One interviewee elaborated, *"It's critical because ultimately with zero trust, when you actually have that sort of access, the perfect world would be that your devices are trusted, you can access from anywhere, you trust your users that are also connecting as well."*

Establish endpoint detection and response (EDR) mechanisms. Experts asserted that organizations should enforce proactive threat detection for endpoints and promptly activate device response mechanisms to block cyber threats and generate alerts. As explained by one interviewee, *"You want to have the right level of detection and response for your endpoints, and you want to be able to protect those endpoints and those devices, regardless of where they're connecting from."*

Another interviewee also consented to this by saying, *"You should be doing that for your corporate assets. You should be doing it for BYOD. And if you're doing it for both of them to a level that says, hang on a sec, if I need more assurance that he is allowed access to this information, you should be raising your levels of assurance regardless of the endpoint."*

4.3. Applications & workload dimension

Applications and workloads in this context consist of computer programs, systems, and services (whether executed on-premises or in the cloud). Organizations have appropriate policies in place to ensure the protection and management of applications and workloads, and to enable a secure application delivery (CISA, 2021).

Enforce adaptive and policy-based access control for applications. As remote work becomes more accepted for most, adaptive access policies should be applied to the application as well. Enterprises are supposed to make access control decisions based on risk appetite through policy engines, such as allowing access and limiting access. One expert remarked, *"It kind of all comes back to access as well, right, because you need your applications to be secure and have the right level of access and people have the right. So, verifying the people that are accessing those applications have the rights to access it. And I have the right level of privilege as well. So it's all sort of in and part of that whole strategy. And obviously from an application development perspective, you want to be securely developing your apps in the perfect world. As part of your software development lifecycle, you're securely embedding security as you develop it so your developers know what they need to adhere to make secure applications."*

Another interviewee from the higher education industry provided an example of this, *"If a student is on the network, they will not be able to actually see all the applications that are on the network. They won't see them or even try to access them. So that's an element of at least need to know, sort of access control or at least privileged access. "*

Monitor and block unauthorized access to applications. One expert pointed out, *"There is access control within the application as well. And the final bit of the access control when it comes to applications is the monitoring of user transactions. So, there's an element of zero trust that comes after the fact in my view. Where can you report and monitor what someone has done on the system? In my view, this fits under the zero trust model and without monitoring, you can't provide an assurance that your zero trust model is working."*

4.4. Infrastructure dimension

Infrastructure can be described as the hardware, software (open source, first-and third-party), microservices (functions, APIs), networking infrastructure, facilities and so forth necessary to develop, test, deliver, monitor, or support IT services, whether local or multi-cloud (Microsoft, 2021a). As infrastructure becomes a critical threat vector, enterprises need to develop comprehensive capabilities to secure it (Microsoft, 2021b).

Manage privileged access. The expert panel stated firmly that managing privileged access is a key step to protect the organizations' critical infrastructure in the zero trust journey. Speaking to this point, an interviewee emphasized that, *"You're essentially ensuring that you're providing the level of trust and security needed to access your infrastructure, whether that's on prem or whether that's in the cloud. So, once you've implemented, in a perfect world, your zero trust strategy and capability to support that. Actually, the infrastructure, the access, the control and the security and the verification are done on the sort of the device and the user. So that in itself means that access in the infrastructure is secure because you've already got that authentication."*

Another expert commented on this view by comparing infrastructure with applications, *"So it's similar to what we do with the applications which is granular access control and also some defence."*

Develop a cloud infrastructure protection plan. Having a comprehensive view across all cloud workloads is critical to keeping organizational resources safe in a highly distributed environment. One interviewee argued that *"You've now got the concept of cloud, you got the concept of PaaS, SaaS, Blob storage. There's a whole load of stuff that comes into play and making sure all that is still taken into account when you build infrastructure and focus on zero trust. It becomes more important as well."*

4.5. Data dimension

In a zero trust environment, data security is primarily concerned with managing data, classifying data, designing data classification schemas, and encrypting data both in transit and at rest (Cunningham, 2018). Data is often the ultimate target for attackers, so the zero trust framework is centred on protecting data. Organizations must understand where data is stored, how it is classified, who has access to it, and monitor and control data access by using policy engines.

Implement data loss prevention (DLP). The expert panel stressed that organizations must take measures to protect user information from malicious or inadvertent disclosure, such as establishing data loss prevention mechanisms. This is corroborated by one participant, *"When it comes to zero trust, you want to make sure that there's no risk of data leakage and that you're sufficiently handling that data as well. So, if people are connecting to cloud applications, you want to make sure that you've got the right level of security. Essentially, you need to ensure that you've got some controls in place, like DLP. So again, data is a fundamental element of the zero trust strategy."*

Govern access decisions based on sensitivity. According to interviewees, the level of protective controls and enforcement is directly proportional to the sensitivity of the data. For example, personal data can be protected by ensuring that only authorized users can access the data through encryption policies. One interviewee shared his views on sensitive data, *"We actually merged our entire strategy to be a data-centric security strategy. And that did a number of really, really beneficial things. It sets the importance of where the value is and indeed the inherent risk is for the organization. In our world, we deal with people's most sensitive of sensitive information."*

This view was echoed by another participant, who suggested that *"There are controls to protect the network. But putting controls on the network and the infrastructure to protect the data can be ineffective in some cases. So, the controls should be closer to the data as much as possible."*

4.6. Networks dimension

The network dimension of a zero trust implementation involves essentially segmentation, isolation, and control of the network. It is considered a crucial point of zero trust strategies because once an attacker has access to the network, they have access to the whole network. Likewise, network segmentation limits the "blast radius" of a potential ransomware attack. Enterprises need to use advanced technology to segment, isolate and control networks to make cyber attacks as difficult as possible (ACT-IAC, 2019). The network perimeter should be as close as possible to the data itself, which drives down to deeper micro-segmentation.

Segment networks. Applying software-defined perimeters with granular controls facilitates limiting the attacker's ability to propagate and spread through the network, thereby greatly reducing the lateral movement of threats and devastating assets after the initial intrusion (Microsoft, 2021a). One interviewee shared a practical example of what his organization has implemented, *"We have technologies in place that enable and allow isolation and segmentation of critical network areas. We can enforce network segmentation with strong security controls such as a next-generation firewall, virtual network infrastructure, or other software-based approaches that strictly enforce access control."*

Encrypt all network traffic. Encrypting network traffic safeguards confidential data in transit from attacks such as man-in-the-middle attacks, eavesdropping, and session hijacking.

As supported by one of the interviewees, *"When it comes to zero trust, because especially with us all working in a distributed fashion now and working from home, obviously there's the sort of overhead that puts on the VPN. And so, when you move into a zero trust architecture, you've got an opportunity to essentially encrypt all network traffic."*

Likewise, one interview highlighted that *"Basically this is based on the fact that, how communication is encrypted from one point to it to the other, right? So, intercepting the communication in transit is not going to provide anyone who intercepts communication with any value because the communication is encrypted, that it's too hard to decrypt that traffic in line."*

4.7. Visibility & analytics dimension

Visibility and analytics refer to making all security-relevant activities occurring in the network visible and understanding them through analytics. Enterprises leverage analytics tools (such as platforms to perform advanced security analysis, security user behaviour analysis) to understand the situation in the network in real time to intelligently defend against and locate attackers. Data analysis of network events can help proactively develop security measures before an actual event occurs (ACT-IAC, 2019).

Ensure visibility and improve situational awareness (Leszczyna et al., 2019; Naderpour et al., 2014). It was proposed by the expert panel that visibility should be achieved by establishing a centralized platform dedicated to investigation, monitoring, and response. An interviewee commented, *"It's crucial. It's absolutely vital. What I normally say to people is you can't manage what you can't see. You need visibility of everything. But the caveat is, once you have that visibility, what you're really talking about is drawing knowledge and insight from that information. So simply having the information is not good enough."*

Another expert added up, *"From the monitoring point of view as well, one is from the usage point of view, so you should have the full landscape view of what's going around in my environment so that I can make better decisions for trend signals, for usage, for monitoring, for any kind of abnormalities."*

Collect threat data and analyse them across other dimensions. Visibility and analysis are based on the other dimensions above (such as identities, endpoints, network, and infrastructure) and it is a by-product of them. The expert panel agreed that visibility and analysis of data help to make effective risk-based decisions. As explained by this interviewee, *"So I would say that visibility and analytics come from all those data points we've just spoken about. It doesn't exist without those other dimensions. I actually don't think it's necessarily a specific dimension. I think it's a by-product of those other data points that we're looking at. We need to be able to see those data points, bring that in, aggregate that information, make decisions or inferences and carry out activities based on that. And of course, if you don't have the visibility where you need, if you have blind spots, we're going to be making risk-based decisions on incomplete data. So, you might not have all the data you need to make the effective decision."*

4.8. Automation & orchestration dimension

Automation and Orchestration comprise the utilization of tools and technologies to automate and orchestrate processes across organizations. Automation and orchestration provide unrivalled capabilities for delivering more efficient and productive security operations, for example, the use of STIX/TAXII systems to automate the transfer and ingestion of Indicators of Compromise (IOC) into intrusion prevention systems. Through automation, organizations can identify and resolve specific threats at an accelerated rate with an accuracy that is unachievable by humans (Netskope, 2020).

Enable automated investigation and response. Automation and scheduling enable machines to perform defined tasks according to defined procedures, thereby increasing efficiency and saving labour. The interviewees believed automated investigation and response mechanisms should be included in zero trust implementation, which will enhance the efficiency of the entire zero trust architecture in terms of execution. One participant highlighted, *"I think automation is essential because with zero trust, you want to make decisions automatically rather than manually."*

Meanwhile, another expert gave an example about this, *"We have around 100,000 devices connecting on the network on any day, sometimes more. Actually, we were averaging 150,000 devices connected on the network last month on a daily basis. So, imagine if this is not automated*

Identity ***Identities are defined as the common dominator across networks, endpoints, and applications, such as people, services, or IoT devices.***	ID1	Internal users (employees) perform multi-factor authentication (MFA) to access all business critical systems/applications/platforms.
	ID2	External users (third parties) perform MFA to access business critical systems/applications/platforms.
	ID3	Single sign-on (SSO) (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate internal users to all critical business systems.
	ID4	Single sign-on (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate external users to all critical business systems.
	ID5	Have a security policy engine to grant access to resources.
	ID6	Identity and access management (IAM) system integrates with privileged access management (PAM).
	ID7	Users are granted only the minimum privileges required for their roles to access resources through continuous verification.
	ID8	Implement role-based access control (RBAC).
	ID9	Real-time user risk and sign-in risk detections are enforced when evaluating access requests.

Fig. 2. CSF Questions for "Identity" Dimension.

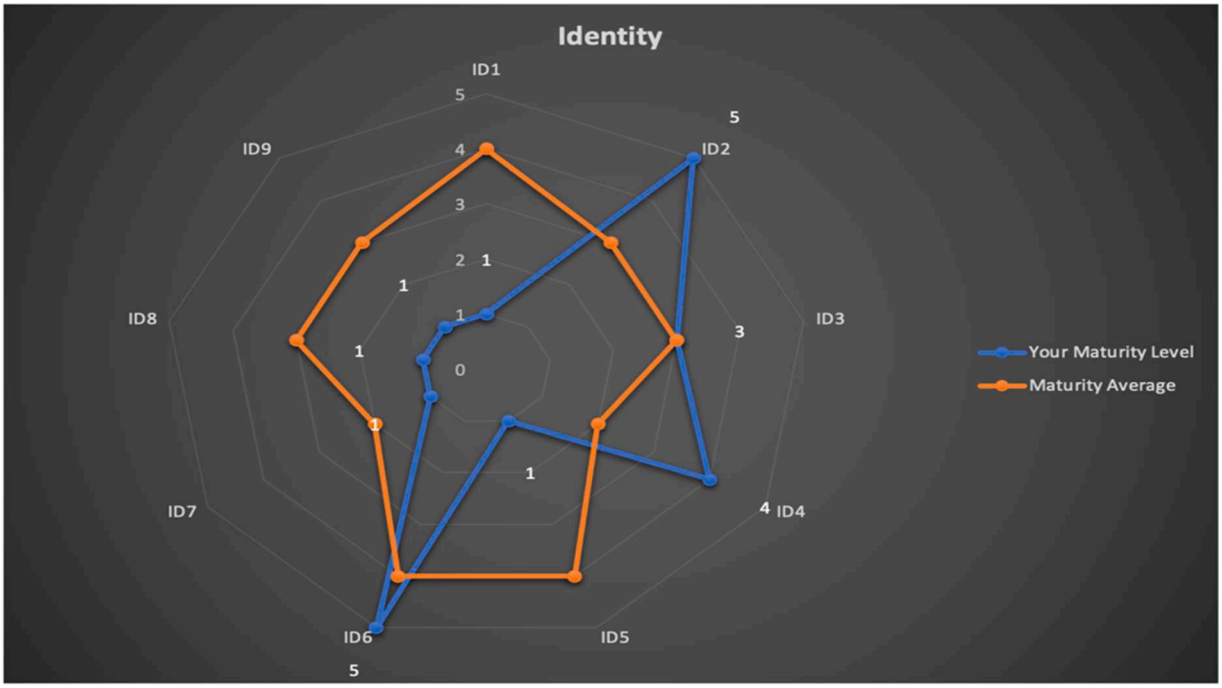

Fig. 3. Visualisation of the Self-Assessment Result for "Identity" Dimension.

decision making, it would be impossible to assess each authentication attempt and determine if this is allowed or not. And the same applies to automating the technology deployment, because this ensures consistency. So, automation also, apart from improving operational effectiveness, it also ensures consistency of how we do certain things and the fact that the policy is always applied."

5. Zero trust maturity assessment framework

Based on the CSFs findings, we develop an operationalizable zero trust maturity assessment framework enabling organizations to assess their zero trust maturity level. The framework consists of two major components: a self-assessment questionnaire (consisting of 43 questions in 8 dimensions) and overall maturity assessment results with visual charts (available at: shorturl.at/muKO6 or in Supplementary Material 2). For example, Fig. 2 depicts a screenshot of the questions for the "identity" dimension. It consists of nine CSF statements in which organizational stakeholders rate the statements using the Likert scale 0 - 5 (0 = not on the roadmap to 5 = completely deployed). The result of self-assessment questionnaire for each dimension is automatically visualized in Fig. 3. After completing all 43 survey questions across the 8 major dimensions, a zero trust maturity assessment report is automatically generated to illustrate the results of maturity levels, as shown in Fig. 4. Fig. 5 outlines maturity scale from 0 to 5 (non-existent, initial, basic, intermediate, advanced and optimised). The framework's user guide, the glossary and the calculation formula are provided in Appendix B, Appendix C and D respectively.

The proposed framework will contribute to a zero trust implementation for organizations in the following ways:

1) Clearly understand the current zero trust maturity level of the organization.
2) Better identify the organization's relative strengths and weaknesses across eight dimensions and determine the focus areas for the organization's zero trust transformation.

Zero Trust Cybersecurity Maturity Level Report

Our framework consists of six Zero Trust maturity levels: Non-existent, Initial, Basic, Intermediate, Advanced and Optimised. According to the results of the completed self-assessment questionnaire, your organization is currently at the Level 2.

Dimension	Maturity Score	Maturity Level	Average Maturity Level	Maturity Gap
Identity	2.37	2	3	-1
Endpoint	2.78	2	3	-1
Application & Workload	3.11	3	2	1
Data	2.86	2	4	-2
Network	2.37	2	3	-1
Infrastructure	3.24	3	4	-1
Visibility & Analytics	2.29	2	2	0
Automation & Orchestration	2.72	2	2	0
Overall	**2.72**	**2**	**3**	**-1**

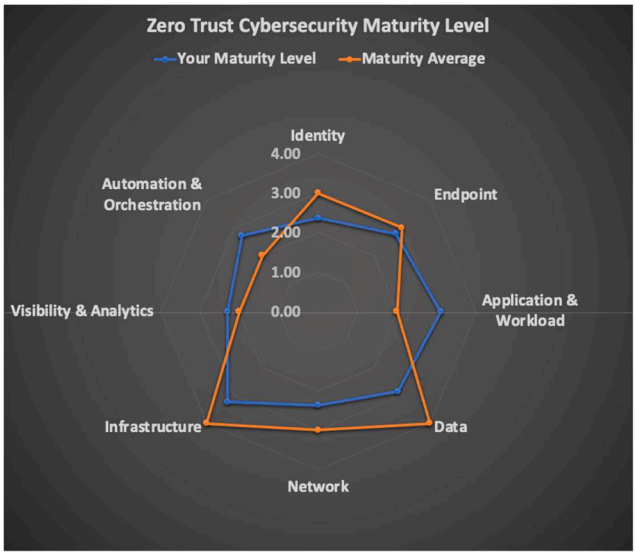

Fig. 4. Zero Trust Maturity Assessment Report.

Level 0 (Non - Existent)

Companies at this level have not yet decided to include zero trust in the roadmap.

Level 1 (Initial)

Zero Trust is on the roadmap. In this preparatory phase, organizations are deploying initial discovery and assessment activities.

Level 2 (Basic)

At this basic level, fundamental zero trust capabilities are implemented. The strategy here is to start small and focus on strategic wins.

Level 3 (Intermediate)

At the intermediate level, the capabilities are further integrated and refined. The strategy at this level is to advance zero trust through more robust identity management, data security, and advanced threat detection and response capabilities.

Level 4 (Advanced)

At this matured level, organizations have deployed advanced controls with robust analytics and orchestration. The strategy for this level is to mature and extend Zero Trust to advance threat intelligence, automation of the SOC, seamless access for end-users and so on.

Level 5 (Optimised)

At this level of optimization, there is an enterprise-wide, integrated, and highly automated approach to zero trust implementation and its monitoring and reporting, which is being refined through continuous improvement.

Fig. 5. Maturity Scale.

3) Comprehensively analyse and visualize what needs to be done to achieve the optimal zero trust implementation.

6. Implications

This paper has several theoretical and practical implications. First, this paper explicitly addresses the theoretical gaps related to zero trust success. Zero trust cybersecurity has received much attention recently in industry, but the study of CSFs for zero trust has so far been neglected. This paper is one of the earliest to contribute towards bridging the gap between industry and academia. We respond to an important topic in the field of zero trust cybersecurity, that is, the contextualization and the operationalization of zero trust success. Using a Delphi approach, we identify and contextualize a set of multidimensional CSFs for zero trust implementation from real-world perspectives. Our research is novel in the sense that no prior empirical study has contextualized the CSFs in the zero trust literature. This paper advances our theoretical understanding of the CSFs for implementing zero trust cybersecurity.

Second, while prior studies have underscored the importance of maturity assessment (Bobbert and Scheerder, 2020), our study has contributed to the body of existing knowledge by developing a maturity assessment framework for evaluating the state of zero trust and for using the assessment results to drive zero trust strategy development. Our assessment framework provides an efficient approach that can be readily operationalized by any organization to assess zero trust maturity, so enabling organizations to better plan, assess, and manage their zero trust undertakings. More specifically, the maturity assessment framework will allow organizations to review and refine their implementation process systematically and rigorously. Additionally, it will assist them in their future strategy formulation, thereby ensuring cost-effective implementation. This maturity assessment framework has not been operationalized in the extant literature to the best of our knowledge.

In terms of practical implications, cybersecurity practitioners and organizational stakeholders can apply our CSFs findings. We present a set of multidimensional CSFs vital for implementing zero trust cybersecurity. The CSFs are real-world insights derived from cybersecurity experts who work as a chief information security officer or equivalent position in multi-billion dollars companies. Organizational stakeholders need to give special and continual attention to those CSFs and allocate corporate resources to support those critical areas because CSFs are those few things that must go well to ensure zero trust success.

Second, based on our theoretical CSF findings, we put forward an operationalized maturity assessment framework for evaluating zero trust cybersecurity maturity in organizations. Businesses and cybersecurity practitioners can readily utilize our operationalized framework to assess their zero trust initiative, which facilitates their planning for more scientific steps to achieve zero trust maturity. Our framework includes structured questionnaires, visual analysis of results, and an overview of organizational maturity. Using the CSF-based maturity assessment framework represents a systematic and promising starting point for understanding and managing zero trust success.

Like all other studies, this paper has limitations that also point the direction for future research. First, this study is a qualitative study utilizing the interview method focusing on replication logic rather than sampling logic. Future studies may adopt quantitative methods such as questionnaire surveys to validate our CSFs findings. Second, the participants in this study were experts from seven sectors in Australia. Future research could increase the diversity of the expert panel by extending this study with experts from different industries in different countries.

7. Conclusion

The strategic shift to implementing zero trust for organizations is a complex and long-lasting undertaking. Utilizing a Delphi method, this research identifies CSFs for implementing zero trust across eight critical dimensions, constituting the first step toward rigorous research in this field. The proposed framework offers organizations a comprehensive guidance on CSFs for zero trust implementation. The combination with the maturity assessment enables organizations to identify the strengths and weaknesses of current zero trust implementations to optimize existing cyber security resource allocations. We hope this work will help future researchers build on this study and stimulate greater interest in research on CSFs for zero trust implementations.

CRediT authorship contribution statement

William Yeoh: Conceptualization, Methodology, Validation, Visualization, Supervision, Writing – original draft, Writing – review & editing. **Marina Liu:** Conceptualization, Methodology, Validation, Visualization, Writing – original draft, Writing – review & editing. **Malcolm Shore:** Conceptualization, Methodology, Writing – review & editing. **Frank Jiang:** Conceptualization, Methodology, Writing – review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The authors do not have permission to share data.

Acknowledgement

We would like to thank Daniel Johns, Principal Security Consultant at MyCISO, for his valuable discussions on our framework and the initial manuscript. We express our gratitude to Deakin University's Centre for Cyber Resilience and Trust (CREST) and the Faculty of Business and Law for funding this project. We also acknowledge Marina Liu's contribution as a research assistant for this project. The intellectual property rights to this work belong solely to Deakin University.

Appendix A: CSFs across 8 dimensions

Fig. A1,Fig. A2,Fig. A3,Fig. A4.

Identity ***Identities are defined as the common dominator across networks, endpoints, and applications, such as people, services, or IoT devices.***	ID1	Internal users (employees) perform multi-factor authentication (MFA) to access all business critical systems/applications/platforms.
	ID2	External users (third parties) perform MFA to access business critical systems/applications/platforms.
	ID3	Single sign-on (SSO) (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate internal users to all critical business systems.
	ID4	Single sign-on (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate external users to all critical business systems.
	ID5	Have a security policy engine to grant access to resources.
	ID6	Identity and access management (IAM) system integrates with privileged access management (PAM).
	ID7	Users are granted only the minimum privileges required for their roles to access resources through continuous verification.
	ID8	Implement role-based access control (RBAC).
	ID9	Real-time user risk and sign-in risk detections are enforced when evaluating access requests.
Endpoint / Devices ***Devices refer to various hardware assets that access data on the Internet, such as smartphones, IoT devices, laptops, bring your own device (BYOD), partner-managed devices, and cloud-hosted servers.***	EN1	All corporate-owned devices (workstations and smart devices) are enrolled by a device enrollment manager.
	EN2	Internal users' smart devices are enrolled in a mobile device management system.
	EN3	Access to corporate resources from external users' smart devices is provided by mobile application management.
	EN4	Both corporate and BYO devices need to be continuously verified before being granted access to corporate resources.
	EN5	Corporate-owned/managed devices are required to be compliant with IT configuration policies before granting access.
	EN6	Real-time endpoint detection and response (EDR) tools are used (e.g., FortiEDR).

Fig. A1. Identity and Endpoint/Devices Dimensions.

Application & Workload ***Applications and workloads consist of computer programs, systems, and services (whether executed on-premises or in the cloud).***	AW1	Workloads are identified and categorised.
	AW2	Policy-based access control on applications is implemented.
	AW3	Session controls policies for your applications are enforced (e.g., limit visibility or block download/upload).
	AW4	Business critical applications are connected to a security platform to continuously monitor cloud threats.
	AW5	Workload behaviour anomalies can be detected.
Data ***In a zero-trust environment, data security is primarily concerned with managing data, classifying data, designing data classification schemas, encrypting data both in transit and at rest (Cunningham, 2018).***	DA1	Data is classified, labelled, and access restricted based on data sensitivity.
	DA2	There is a cloud security policy engine to help make data access decisions.
	DA3	Business critical/sensitive data at rest is encrypted.
	DA4	Business critical/sensitive data in transit is encrypted.
	DA5	There are data loss prevention (DLP) controls in place to monitor, alert, or restrict the flow of sensitive information (e.g., blocking email, uploads, or copying to USB).
	DA6	The authorisation of data access is controlled via a request and approval process.
	DA7	A formalised data governance program that includes continually managing and maintaining data schemas is employed.

Fig. A2. Application & Workload and Data Dimensions.

Network ***The network dimension of a zero trust implementation involves essentially segmentation, isolation, and control of the network.***	NE1	Micro-segmentation is implemented for network environment.
	NE2	Enforces access restrictions based on the context of access requests.
	NE3	Encrypt all network traffic (e.g., using digital certificates).
	NE4	Ingress and Egress points of the network are protected by a next-generation firewall.
Infrastructure ***Infrastructure can be described as the hardware, software (open source, first-and third-party), microservices (functions, APIs), networking infrastructure, facilities and so forth necessary to develop, test, deliver, monitor, or support IT services, whether local or multi-cloud (Microsoft, 2021).***	IN1	Understand the risk profile of your cloud architecture and develop a cloud infrastructure protection plan.
	IN2	Have the capability to detect and quickly respond to security incidents (SIEM) in a cloud architecture.
	IN3	Access to cloud services is protected by a secure web gateway (SWG).
	IN4	Employ a vulnerability management solution to ensure that security vulnerabilities are identified on any infrastructure device and patched within a prescribed time frame (e.g., 48 hours).

Fig. A3. Network and Infrastructure Dimensions.

Visibility & Analytics ***Visibility and analytics refer to making all security-relevant activities occurring in the network visible and understanding them through analytics.***	VA1	Regularly use network discovery tools, flow analysis tools, or packet capture tools to capture and analyse netowrk traffic.
	VA2	Apply network metadata analysis tools (e.g., LogRhythm NetworkXDR, Awake, Corelight).
	VA3	Perform real-time device risk analysis integrated with user behavior analytics (UBA).
	VA4	Have security operations center (SOC) analysts monitoring 24/7.
Automation & Orchestration ***Automation and Orchestration comprise the utilization of tools and technologies to automate and orchestrate processes across organizations.***	AO1	Use automated tools or techniques to manage and control network segmentation.
	AO2	Implement automated data classification and labeling.
	AO3	Automate anomaly detection.
	AO4	Automate remediation actions for security incidents.

Fig. A4. Visibility & Analytics and Automation & Orchestration Dimensions.

	To what extent has your organization deployed the following Critical Success Factor (CSF) statements?	Why does your organization need to deploy the following CSF statements?	NIST CSF	ISO/IEC 27001	ACSC Essential Eight	Your Answer (0 = Not on roadmap 1 = On roadmap 2 = Deployment scoped 3 = Partially deployed 4 = Mostly deployed 5 = Completely deployed)	Matu
ID1	Internal users (employees) perform multi-factor authentication (MFA) to access all business critical systems/applications/platforms.	MFA is a efficient way to enhance the security of internal user accounts by reducing the attacks associated with compromised passwords, such as brute force, credential stuffing.	PR.AC-7	A.1 - 8.5	Multi-factor authentication	1	
ID2	External users (third parties) perform MFA to access business critical systems/applications/platforms.	MFA is a efficient way to enhance the security of external user accounts by reducing the attacks associated with compromised passwords, such as brute force, credential stuffing.	PR.AC-7	A.1 - 8.5	Multi-factor authentication	5	
ID3	Single sign-on (SSO) (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate internal users to all critical business systems.	SSO can elevate user experience, improve productivity of internal users by logging in at regular intervals (often once a day) and revamp security by decreasing the number of attack surfaces.		A.1 - 8.5		3	
ID4	Single sign-on (e.g., Azure Active Directory (AAD), Okta, etc) is used to authenticate external users to all critical business systems.	SSO can elevate user experience, save time of external users by logging in at regular intervals (often once a day) and revamp security by decreasing the number of attack surfaces.		A.1 - 8.5		4	
ID5	Have a security policy engine to grant access to resources.	The policy engine is an important component to determine whether to grant access to a resource by monitoring and enforcing specific rules.	PR.AC-6	A.1 - 5.15		1	
ID6	Identity and access management (IAM) system integrates with privileged access management (PAM).	The integration of IAM and PAM can save time and simplify the process of protecting the identity of all users.		A.1 - 8.2		5	
ID7	Users are granted only the minimum privileges required for their roles to access resources through continuous verification.	Enforcing least privilege and continuous verification are instrumental in effectively managing privileges.	PR.AC-4	A.1 - 8.2	Restrict administrative privileges	1	
ID8	Implement role-based access control (RBAC).	Role-based access control (RBAC) makes sure that users have varying levels of access rights depending on their role.	PR.AC-4	A.1 - 8.3		1	
ID9	Real-time user risk and sign-in risk detections are enforced when evaluating access requests.	Risk can be detected in a timely manner so that organizations can quickly respond to suspicious behavior.	DE.CM-1, DE.CM-3			1	

0 1 2 3 4 5

Fig. B1. Entering Answers.

Appendix B: zero trust maturity assessment framework user guide

Fig. B1,Fig. B2,Fig. B3

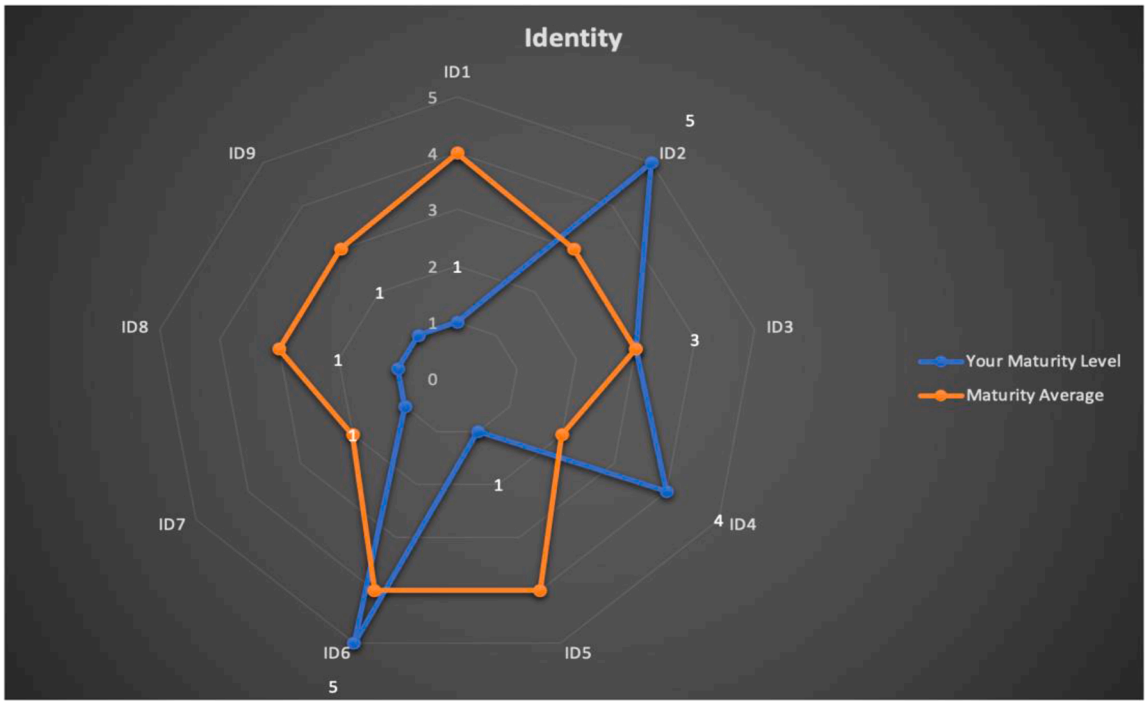

Fig. B2. Visualisation of the Self-Assessment Result for "Identity" Dimension.

Zero Trust Cybersecurity Maturity Level Report

Our framework consists of six Zero Trust maturity levels: Non-existent, Initial, Basic, Intermediate, Advanced and Optimised. According to the results of the completed self-assessment questionnaire, your organization is currently at the Level 2.

Dimension	Maturity Score	Maturity Level	Average Maturity Level	Maturity Gap
Identity	2.37	2	3	-1
Endpoint	2.78	2	3	-1
Application & Workload	3.11	3	2	1
Data	2.86	2	4	-2
Network	2.37	2	3	-1
Infrastructure	3.24	3	4	-1
Visibility & Analytics	2.29	2	2	0
Automation & Orchestration	2.72	2	2	0
Overall	**2.72**	**2**	**3**	**-1**

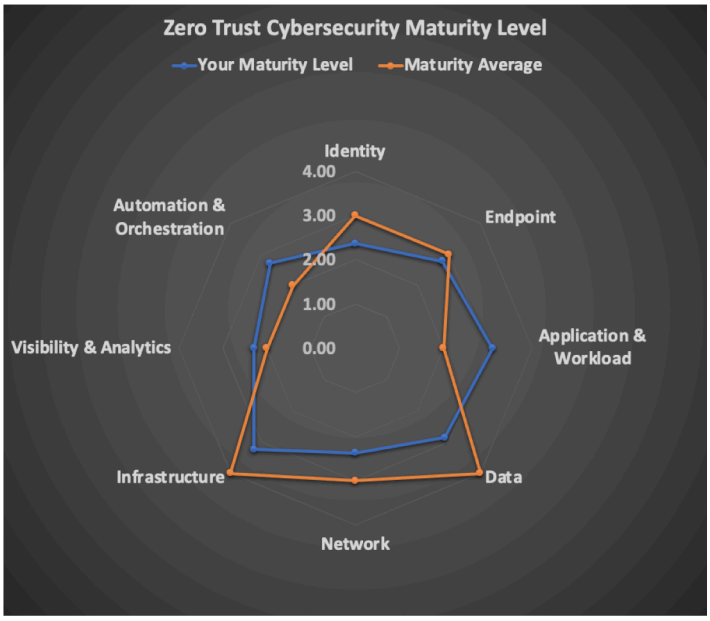

Fig. B3. Zero Trust Maturity Assessment Report.

Step 1:

Enter your answer in the specified cell (Maturity Level Questionnaire => Column I) next to each question. Each question needs to be answered with any number from a Likert scale of 0 - 5 (0 = not on the roadmap, 1 = on the roadmap, 2 = deployment scoped, 3 = partially deployed, 4 = mostly deployed, 5 = completely deployed).

Step 2:

Visual charts for each dimension are automatically generated after you answer the questions. It illustrates your maturity level and the average maturity level for a certain dimension.

Step 3:

Get your maturity assessment results on the "Report" tab.

Appendix C: Glossary

Table C1

Table C1
Concepts and explanations.

Concept	Explanation
Critical Success Factor (CSF) Statement	CSFs are things that must be done to achieve success (Freund, 1988). In this study, it refers to the controls that an enterprise should deploy to achieve a successful zero trust implementation.
Maturity Level	The extent to which your organization has deployed the given CSF statements of zero trust implementation.
Average Maturity	The average of the maturity levels of all companies that have used the proposed tool.
Maturity Gap	The difference between a company's actual zero trust implementation maturity level and the industry average maturity level.
Maturity Weight	A value given to each CSF statement based on its importance to zero trust implementation.

Appendix D: Calculation formula

$$\text{Maturity Level(Dimension)} = \frac{Sum\ of\ (User\ Input\ Maturity\ Weight)\ in\ a\ Given\ Dimension}{Sum\ of\ All\ the\ Maturity\ Weights\ in\ a\ Given\ Dimension}$$

$$\text{MaturityLevel(Total)} = \frac{Sum\ of\ Maturity\ Level\ (Dimension)}{Number\ of\ Dimensions}$$

References

ACT-IAC, 2019. Zero Trust Cybersecurity Current Trends. American Council for Technology-Industry Advisory Council (ACT-IAC). https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends.

Adahman, Z., Malik, A.W., & Anwar, Z., 2022. An analysis of zero-trust architecture and its cost-effectiveness for organizational security. Comput. Secur., 122, 102911. 10.1016/j.cose.2022.102911.

Adeoye-Olatunde, O.A., Olenik, N.L., 2021. Research and scholarly methods: semi-structured interviews. JACCP 4 (10), 1358–1367. https://doi.org/10.1002/jac5.1441.

Bennett, M., Balaouras, S., & Glenn, M. (2017). Zero Trust Security: A CIO's Guide To Defending Their Business From Cyberattacks. F. Research. https://www.forrester.com/report/zero-trust-security-a-cio-s-guide-to-defending-their-business-from-cyber attacks/RES136651?ref_search=0_1647411000276.

Bobbert, Y., Scheerder, J., 2020. Zero trust validation: from practical approaches to theory. Sci. J. Res. Rev. 2 (5) https://doi.org/10.33552/SJRR.2020.02.000546.

Bogner, A., & Menz, W., 2009. The theory-generating expert interview: epistemological interest, forms of knowledge, interaction. In Interviewing Experts (pp. 43–80). Palgrave Macmillan. 10.1057/9780230244276_3.

Braun, V., Clarke, V., 2019. Reflecting on reflexive thematic analysis. Qual. Res. Sport Exerc. Health 11 (4), 589–597. https://doi.org/10.1080/2159676X.2019.1628806.

Buck, C., Olenberger, C., Schweizer, A., Völter, F., Eymann, T., 2021. Never trust, always verify: a multivocal literature review on current knowledge and research gaps of zero-trust. Comput. Secur. 110, 102436 https://doi.org/10.1016/j.cose.2021.102436.

Campbell, M., 2020. Beyond zero trust: trust is a vulnerability. Computer (Long Beach Calif) 53 (10), 110–113. https://doi.org/10.1109/MC.2020.3011081.

CISA. (2021). Zero Trust Maturity Model. C. a. I. S. Agency. https://www.cisa.gov/zero-trust-maturity-model.

Creswell, J.W., Creswell, J.D., 2018. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (Fifth ed.) [Bibliographies]. SAGE Publications, Inc. https://ezproxy.deakin.edu.au/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=cat00097a&AN=deakin.b4437699&site=eds-live&scope=site.

Cunningham, C. (2018). The Zero Trust eXtended (ZTX) Ecosystem. Forrester. https://engage2demand.cisco.com/LP=10091.

Cunningham, C., Holmes, D., Pollard, J., 2019. The eight business and security benefits of zero trust. F. Reseach. https://www.forrester.com/report/the-eight-business-and-security-benefits-of-zero-trust/RES134863?objectid=RES134863.

Deloitte. (2021). A revolutionary approach to Cyber or just another buzz word? https://www2.deloitte.com/uk/en/pages/risk/articles/zero-trust.html.

Egfjord, K.F.-H., Sund, K.J., 2020. A modified Delphi method to elicit and compare perceptions of industry trends. MethodsX 7, 1–10. https://doi.org/10.1016/j.mex.2020.101081.

Ferretti, L., Magnanini, F., Andreolini, M., Colajanni, M., 2021. Survivable zero trust for cloud computing environments. Comput. Secur. 110, 102419 https://doi.org/10.1016/j.cose.2021.102419.

Freund, Y.P., 1988. Critical success factors. Plan. Rev. 16 (4), 20–23. https://doi.org/10.1108/eb054225.

Golden, D., Perinkolam, A., Nicholson, M., Rafla, A., & Norton, K. (2021). Zero trust: never trust, always verify. Deloitte. https://www2.deloitte.com/us/en/insights/focus/tech-trends/2021/zero-trust-security-framework.html.

Hasson, F., Keeney, S., McKenna, H., 2000. Research guidelines for the Delphi survey technique. J. Adv. Nurs. 32 (4), 1008–1015. https://doi.org/10.1046/j.1365-2648.2000.t01-1-01567.x.

Jakkal, V. (2021). Zero Trust Adoption Report: how does your organization compare? Microsoft. https://www.microsoft.com/security/blog/2021/07/28/zero-trust-adoption-report-how-does-your-organization-compare/.

Kerman, A., Borchert, O., Rose, S., Division, E., & Tan, A. (2020). Implementing a Zero Trust Architecture. N. I. o. S. a. T. (NIST). https://csrc.nist.gov/publications/detail/white-paper/2020/10/21/implementing-a-zero-trust-architecture/final.

Leszczyna, R., Wallis, T., Wróbel, M.R., 2019. Developing novel solutions to realise the European Energy – information sharing & analysis centre. Decis. Support Syst. 122, 113067 https://doi.org/10.1016/j.dss.2019.05.007.

Meuser, M., Nagel, U., 2009. The expert interview and changes in knowledge production. In: Interviewing Experts, 39. Palgrave Macmillan, pp. 17–42.

Microsoft. (2021a). The 2021 Microsoft Digital Defense Report. https://info.microsoft.com/ww-landing-Microsoft-Digital-Defense-Report-Gate.html.

Microsoft. (2021b). Evolving Zero Trust. Microsoft. https://www.microsoft.com/en-us/security/business/zero-trust.

Naderpour, M., Lu, J., Zhang, G., 2014. An intelligent situation awareness support system for safety-critical environments. Decis. Support Syst. 59, 325–340. https://doi.org/10.1016/j.dss.2014.01.004.

Netskope. (2020). Zero Trust Leading Practice. Netscope. https://resources.netskope.com/cloud-security-solution-white-papers/zero-trust-leading-practice.

Okoli, C., Pawlowski, S.D., 2004. The Delphi method as a research tool: an example, design considerations and applications. Info. Manage. 42 (1), 15–29. https://doi.org/10.1016/j.im.2003.11.002.

Sciarretta, G., Carbone, R., Ranise, S., Viganò, L., 2020. Formal analysis of mobile multi-factor authentication with single sign-on login. ACM Trans. Privacy Security (TOPS) 23 (3), 1–37. https://doi.org/10.1145/3386685.

Turner, S., Holmes, D., Cunningham, C., Budge, J., McKay, P., Cser, A., Shey, H., & Maxim, M. (2021). A Practical Guide To A Zero Trust Implementation. Forrester. https://www.forrester.com/report/a-practical-guide-to-a-zero-trust-implementation/RES157736.

Ward, R., & Beyer, B., 2014. Beyondcorp: A new approach to enterprise security.;login., 39(6), 6–11.
Yeoh, W., Huang, H., Lee, W.S., Al Jafari, F., Mansson, R., 2021. Simulated phishing attack and embedded training campaign. J. Comput. Info. Syst. 1–20. https://doi.org/10.1080/08874417.2021.1919941.
Yeoh, W., Koronios, A., 2010. Critical success factors for business intelligence systems. J. Comput. Inf. Syst. 50 (3), 23–32. https://doi.org/10.1080/08874417.2010.11645404.

William Yeoh is an Associate Professor at Deakin Business School, Deakin University. He also serves as an Innovation Lead at Deakin's Centre for Cyber Resilience and Trust (CREST). His scholarship has been published in leading journals and top information systems conference proceedings (i.e., ICIS, HICSS), and has been supported by various funding bodies and industries. He has been recognised for excellence in teaching, research, and service, receiving Educator of the Year Gold Award (a national award from the Australian Computer Society ACS), Deakin Vice-Chancellor's Award for Value Innovation, Deakin Faculty Research Excellence Award, and two-time internationally-competitive IBM Faculty Awards.

Marina Liu is a PhD candidate at Deakin University. She received her master's degree in cyber security from Deakin University in 2021. Her current research interests include cyber security management, zero trust security, operational technology and IoT security.

Malcolm Shore is an Adjunct Professor at the Centre for Cyber Resilience and Trust at Deakin University. He was instrumental in developing and launching the vocational Certificate IV in Cybersecurity throughout Australia. He is the author of numerous online cybersecurity and programming courses published through LinkedIn Learning and Offsec. He has published research and presented at conferences in the cybersecurity field on topics including cryptography, information warfare, trustworthy systems, survivable networks and 5 G mobile security. His-current research areas include zero trust and cybersecurity training through contemporary approaches to red-blue exercises.

Frank Jiang is a Senior Lecturer in Cyber Security at the School of IT at Deakin University. He completed his PhD degree in communication and cyber security at University of Technology Sydney and won the prestigious UNSW Vice-Chancellor's Postdoctoral Research Fellowship. His research interests include IoT security and privacy, embedded hardware motes, intrusion detection, blockchain-based supply chain, and bio-inspired context-aware algorithms and protocols. He holds an Australian patent in IDS security as the first inventor, and has published over 200 articles in highly respected SCI/EI journals and conferences (with an H-index of 20), including venues like IEEE Trustcom, AAAI, ICDM, BIBM, ICSOC, WCCI, ACM Computing Surveys, KBS, IEEE TIFS.