ISSN: 2687-8097

Scientific Journal of Research and Reviews

DOI: 10.33552/SJRR.2020.02.000546

Iris Publishers

Research Article

Zero Trust Validation: From Practical Approaches to Theory

Yuri Bobbert[1]*, Jeroen Scheerder[2]

[1]ON2IT, Antwerp Management School, Netherlands

[2]ON2IT, Netherlands

*Corresponding author: Yuri Bobbert, ON2IT, Antwerp Management School, Netherlands.

Received Date: May 25, 2020

Published Date: June 26, 2020

Abstract

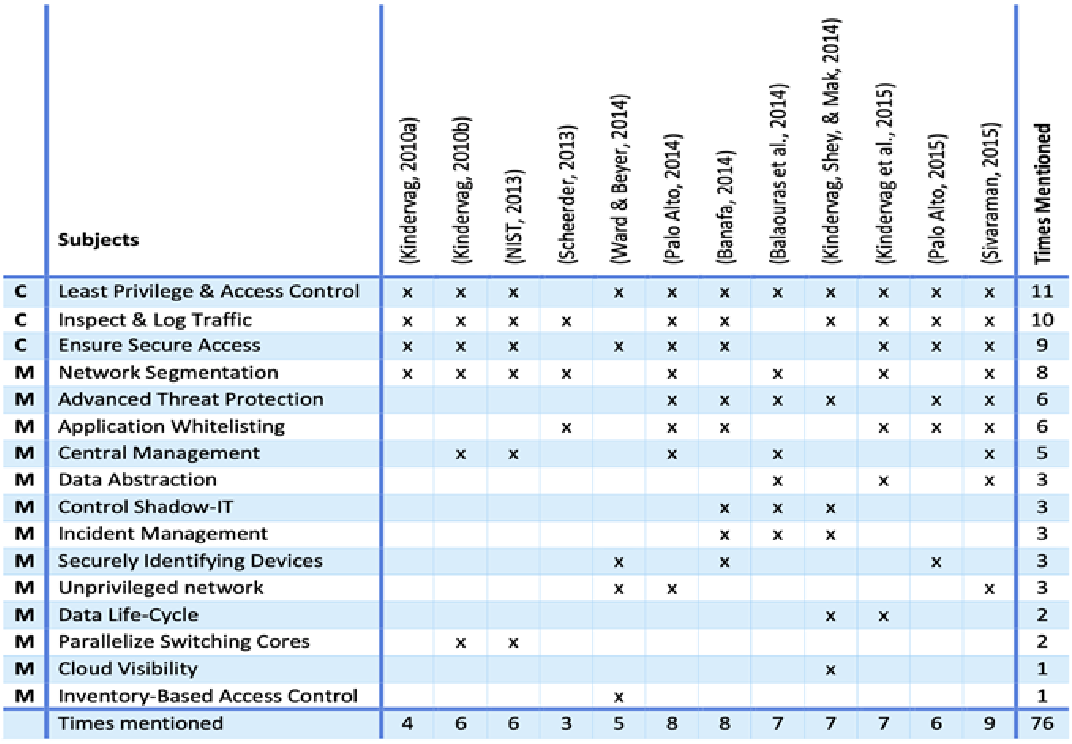
How can high-level directives concerning risk, cybersecurity and compliance be operationalized in the central nervous system of any organization above a certain complexity? How can the effectiveness of technological solutions for security be proven and measured, and how can this technology be aligned with the governance and financial goals at the board level? These are the essential questions for any CEO, CIO or CISO that is concerned with the wellbeing of the firm. The concept of Zero Trust (ZT) approaches information and cybersecurity from the perspective of the asset to be protected, and from the value that asset represents. Zero Trust has been around for quite some time. Most professionals associate Zero Trust with a particular architectural approach to cybersecurity, involving concepts such as segments, resources that are accessed in a secure manner and the maxim "always verify never trust". This paper describes the current state of the art in Zero Trust usage. We investigate the limitations of current approaches and how these are addressed in the form of Critical Success Factors in the Zero Trust Framework developed by ON2IT 'Zero Trust Innovators' (1). Furthermore, this paper describes the design and engineering of a Zero Trust artifact that addresses the problems at hand (2), according to Design Science Research (DSR). The last part of this paper outlines the setup of an empirical validation trough practitioner oriented research, in order to gain a broader acceptance and implementation of Zero Trust strategies (3). The final result is a proposed framework and associated technology which, via Zero Trust principles, addresses multiple layers of the organization to grasp and align cybersecurity risks and understand the readiness and fitness of the organization and its measures to counter cybersecurity risks.

Keywords: Zero Trust Strategy, Design Science Research, Zero Trust Readiness, Artefact design and development

Introduction

Nowadays platform oriented businesses are built on api-based-ecosystems of data, assets, applications and services. These hybrid technology landscapes, most of the time built on clouds, lack real-time visibility and control when it comes to their operations [1]. This makes it hard for boards to take ownership and accountability of cyber risks [2]. Standardized frameworks such as the ISO27000 are being applied in order to implement Information Security. According to Siponen [3] "these frameworks are generic or universal in scope and thus do not pay enough attention to the differences between organizations and their information security requirements". In practice we have seen the application of frameworks falter because they tend to become a goal on their own rather than a supporting frame of reference to start dialogues with key stakeholders. Kluge et al. [4] for example also noted that the use of frameworks as a goal on its own does not support the intrinsic willingness and commitment to improve. This is especially the case for mid-market organizations that lack dedicated security staff, capabilities and / or sufficient budgets. Puhakainen and Siponen [5] noted that information security approaches are lacking not only theoretically grounded methods, but also empirical evidence of their effectiveness. Many other researchers [6-8] have also pointed out the necessity of empirical research into practical interventions and preconditions in order to support organizations with improving the effectiveness of their security. These theoretical voids, as well as the practical observation of failing compliant-oriented approaches, widen the knowledge gap [9]. This "knowing-doing gap" [10] is also perceived in the current Zero Trust approaches which predominantly aim at the technology or by the technology industry. A query on the RSA Conference[1] website in February 24th resulted in 178 items ranging from presentations to exhibitors. With vendors like; Appgate, Centrify, Cisco, Microsoft[2], Palo Alto Networks[3], Truefort, Menlo, Illumio, Mobile Iron, Entrust, Pulse Secure etc. all positioning Zero Trust. Thus, presence of the Zero Trust in the practitioner's community is widely represented. In 2015 The National Institute of Standards and Technology (NIST) as part of the U.S. Department of Commerce drafted the first and second draft of the NIST Special Publication (SP) 800-207, Zero Trust Architecture (ZTA), which discusses the core logical components that make up a zero trust architecture (ZTA) network strategy[4]. The second draft publication builds upon the first draft with a new section on zero trust approaches as well as updates to material based on public comments. Antwerp University, ING Bank and ON2IT contributed extensively on these comments to improve Zero Trust implementations. ON2IT commented based on over 10 years of experience with implementing Zero Trust implementations. One of the public reference cases for the ZT approach and successful implementation is Damen Shipyards, a global yacht and ship constructor which operates in multiple continents with various regulator and security risk requirements. These contributions predominantly arise from practitioners and very little from academia. Some efforts were made in the past when de-parameterization was coined as Jericho[5] [11]. But the academic research is limited compared to other business or information sciences. Researcher Modderkolk [12] examined the academic knowledge base and found "only" 4 out of 12 papers as peer reviewed via the academic rigor, see table. Modderkolk's research distinguished 16 subjects, derived from 12 papers, to utilize via technology to improve Zero Trust maturity. By this vendor tech focus and limited amount of academic publications we can assume that the Zero Trust concept is under highlighted in the scientific world and appear to exist predominantly in the technology vendor space and more precisely in the silo of engineering and architecture (Table 1).

Table 1: Zero Trust subjects mentioned in literature (taken from Modderkolk).



	Subjects	(Kindervag, 2010a)	(Kindervag, 2010b)	(NIST, 2013)	(Scheerder, 2013)	(Ward & Beyer, 2014)	(Palo Alto, 2014)	(Banafa, 2014)	(Balaouras et al., 2014)	(Kindervag, Shey, & Mak, 2014)	(Kindervag et al., 2015)	(Palo Alto, 2015)	(Sivaraman, 2015)	Times Mentioned
C	Least Privilege & Access Control	x	x	x		x	x	x	x	x	x	x	x	11
C	Inspect & Log Traffic	x	x	x	x		x	x		x	x	x	x	10
C	Ensure Secure Access	x	x	x		x	x	x			x	x	x	9
M	Network Segmentation	x	x	x	x		x		x		x		x	8
M	Advanced Threat Protection						x	x	x	x		x	x	6
M	Application Whitelisting				x		x	x			x	x	x	6
M	Central Management		x	x			x		x				x	5
M	Data Abstraction								x		x		x	3
M	Control Shadow-IT							x	x	x				3
M	Incident Management							x	x	x				3
M	Securely Identifying Devices					x		x				x		3
M	Unprivileged network					x	x						x	3
M	Data Life-Cycle									x	x			2
M	Parallelize Switching Cores		x	x										2
M	Cloud Visibility									x				1
M	Inventory-Based Access Control					x								1
	Times mentioned	4	6	6	3	5	8	8	7	7	7	6	9	76

[1] The RSA Conference is a series of IT security conferences. Approximately 45,000 people attend one of the conferences each year (Source wikipedia.org). It is the leading cyber-industry conference held. Source: https://www.rsaconference.com/site-search?q=zero%20trust

[2] Microsoft released the "Zero Trust Maturity Model" (to measure the implementation and readiness for Zero Trust and focusses on the implementation and use of Microsoft technology over 6 foundational elements; identities, devices, applications, Data, infrastructure, networks.

[3] Palo Alto Networks released the "Zero Trust Maturity Model". Designed using the Capability Maturity Model, the Zero Trust Maturity Model mirrors the 5-step methodology for implementing Zero Trust and should be used to measure the maturity of a single Protect Surface. (https://www.paloaltonetworks.com/resources /guides/ zero-trust-maturity-model)

[4] https://www.nist.gov/news-events/news/2019/09/zero-trust-architecture-draft-nist-sp-800-207-available-comment.

[5] The Jericho Forum was an international group working to define and promote de-perimeterization. It was initiated by David Lacey from the Royal Mail, and grew out of a loose affiliation of interested corporate CISOs (Chief Information Security Officers). It declared success, and merged with The Open Group industry consortium's Security Forum in 2014.

Problem

Since Zero Trust predominantly is being viewed, examined and practiced by technicians and architects, it has gained little attention at senior management and board level. According to Jagasia "Zero-Trust does not require adoption of any new technologies. It's simply a new approach to cybersecurity to "never trust, always verify," or to eliminate any and all trust, as opposed to the more common perimeter-based security approach that assumes user identities have not been compromised, all human actors are responsible and can be trusted" [13]. Although the term "Zero Trust" can be perceived that individuals as human beings cannot be trusted, Zero Trust actually implies humans can be trusted but always need to be verified before access and authorization is granted. Jagasia quotes; "*perimeter-based security primarily follows* "*trust and verify,*" which is fundamentally different from ZTA's paradigm shift of "verify, and then trust." Kindervag formulates it more strongly: we have to get rid of the concept of trust: "*The point of Zero Trust is not to make networks, clouds, or endpoints more trusted; it's to eliminate the concept of trust from digital systems altogether. Kindervag proceeds with; "We've injected this concept of trust into digital systems, but it should have never been there, because trust represents a vulnerability for digital systems*". [14].

Over the years, research and consulting companies developed and implemented their own internally developed approaches based upon accepted community frameworks like COSO for Enterprise Risk Management (ERM), COBIT for governing IT (Enterprise Governance of IT, EGIT) and ISO because of it's respected position in quality assurance in retail and industrial environments. The ISO27000 series is already a predominant factor in information security management when it comes to ensuring the Plan, Do, Check, Act cycle that is needed for maintaining an adequate improvement cycle and ISO27002 for the required security controls per domain. Since its introduction in 2010, research and consulting firm Forrester put forward the thought leadership of John Kindervag [14] in their approaches, mainly focusing on managerial level but lack operational detailing that DevOps teams and engineers can get proper guidance from. Most of the security measures are derived from the control objectives in control frameworks and are not directly aligned to security measures prescribed by tech vendors. Consequently, linking the strategic objectives to operational security measures is complex and rarely takes place [8]. The problem with an approach that lacks alignment with strategic goals, lays in the limitations of mainly IT-focused security and security experts working in silos with limited view on the world and the business drivers and context [9]. This is important, as information security is subject to many different interpretations, meanings and viewpoints [15], especially since major breaches can have serious impact on the continuity of the firm as well as their individual board members [16]. Bobbert states in his research into improving Business information security that it needs to be a collaborative effort between Technology, Business (Asset Owners) and risk management to establish and maintain a proper and -near- real time Cyberrisk and security administration.

According to NIST (2019) publications Zero Trust misses a common framework or alignment with existing frameworks- and a common vocabulary. This works both ways. Operational IT-staff needs strategic guidance to implement Zero Trust. Boards need to know what knowledge and capabilities are required to turn knowledge into action[6]. And by doing that cross the bridge of what should be done, according to the high-level frameworks, and that what is actually in place in the operations in terms of capabilities (e.g. measures, checks and balances) that proof effectiveness. According to Pfeffer and Suttons publication "How Smart Companies Turn Knowledge into Action", crossing this "Knowing-Doing Gap" effectively makes organizations outperform their peers [10]. To effectively link the strategic level of the organization to the operational level in the organization, we need to have a proper level of awareness and understanding on how to do this. We explore this challenge based on earlier research in this domain, distinguishing per organizational level the processes and data (Figure 1).

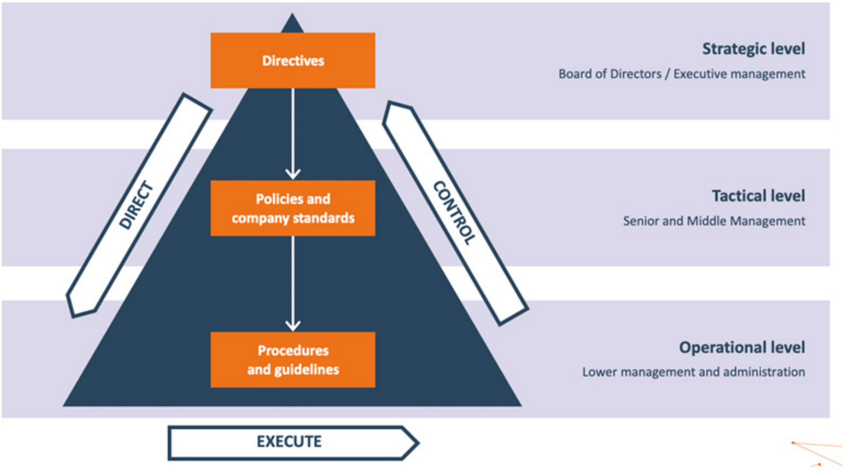

Directives
Strategic level
Board of Directors / Executive management
DIRECT
CONTROL
Policies and company standards
Tactical level
Senior and Middle Management
Procedures and guidelines
Operational level
Lower management and administration
EXECUTE

Figure 1: The IS Governance Direct Control Cycle taken from Von Solms and Von Solms and used in COBIT5 as EDM.

[6] Hooper et al. states "organizations need to embrace their concern about cybersecurity and build it into their selection criteria for board members"

Business Information Security processes and data

The key Information Security Governance layers of information risk and security to cross this knowing doing gap and to gain this integral view Von Solms and Von Solms developed the Direct Control Cycle [17] where they distinguish three organizational levels, Governance, Management and Operational level.

We will describe each of the 3 organizational levels with some examples. The directive-setting objectives come from the strategic level. The risk appetite and accompanying policies are communicated to senior management in the form of requirements. Senior management is then mandated to put these policies into standards (e.g. technical, human and process requirements). These standards are applied in terms of all kind of risks (e.g. through maintenance of risk logs) and security (e.g. security action plans, advisories) processes and controls (e.g. general IT controls). These processes and controls rely on underlying processes such as service processes, change management processes and operational processes with clear requirements, such as firewall rule verifications, log handling, etc.

Most of these processes and their underlying measures are semi or fully automated, once configured properly. Some examples are Technical State Compliance Monitoring (TSCM), Vulnerability management (VM), Intrusion Prevention Systems (IPS), Security Information and Event Management (SIEM), Data Leakage Prevention (DLP), Threat Intelligence (TI), Secure Software Development (SSD) and Penetration Testing.

All security requirements that are needed to keep risks within the risk appetite boundaries are stored in data repositories and documents such as Business Impact Analysis (BIA), Operational Security Guidelines (OSG), Security Requirement Lists (SRL) etc. a detailed meta model is shown in the entire research book of Bobbert (2018) [18]. Due to changes in legislation, technology and business environment these requirements frequently change. In most organizations, documents reside on SharePoint servers, desktops and end-user computers (mobile devices) in spreadsheets [19]. This makes it an administrative burden to maintain a single location for such records and documentation management becomes a risk on its own since there is no single place of truth [20].

This problem increases with the growth of the Internet of Things, changes in technology, software-based devices and emerging cyber threats. Regulated companies, such as financial institutions, do better in this respect, since managing information risk and security is part of their license to operate and they tend to allocate sufficient resources for it, such as dedicated security departments with dedicated Governance, Risk and Compliance (GRC) tools [21]. Smaller, mid-market organizations struggle with this [22]. Within IT operations numerous security and service management processes are active in order to maintain a certain level of operational security control, given the information risks that may arise. All these processes provide input on the performance and compliance of information risk and security management. Prioritizing and selecting the appropriate parameters that reflect the relevant operational data for the right audience is a cumbersome task. This requires collaboration between a number of stakeholders and target groups at the three organizational levels. Continuous measurement and reporting on the performance of risk and security processes is needed in order for boards and executive management to maintain control over BIS (Figure 2).

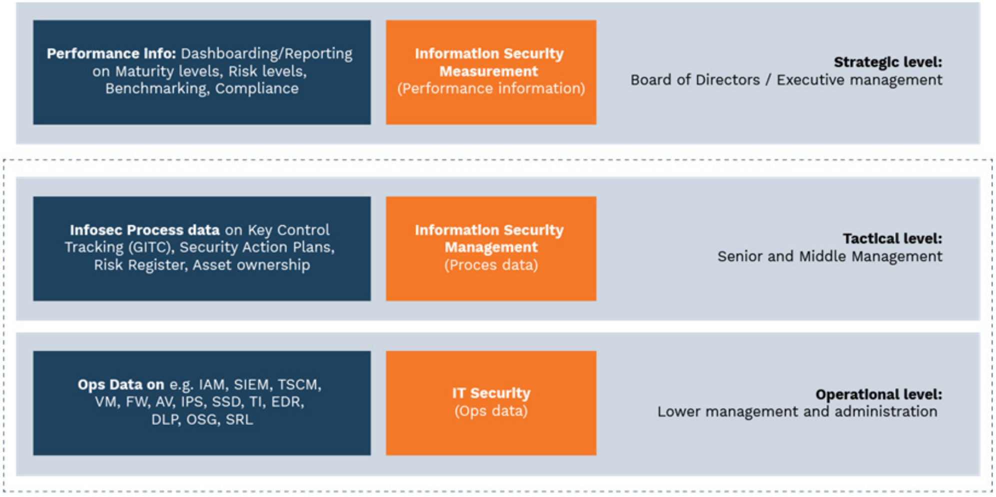

Performance Info: Dashboarding/Reporting on Maturity levels, Risk levels, Benchmarking, Compliance
Information Security Measurement (Performance information)
Strategic level: Board of Directors / Executive management
Infosec Process data on Key Control Tracking (GITC), Security Action Plans, Risk Register, Asset ownership
Information Security Management (Proces data)
Tactical level: Senior and Middle Management
Ops Data on e.g. IAM, SIEM, TSCM, VM, FW, AV, IPS, SSD, TI, EDR, DLP, OSG, SRL
IT Security (Ops data)
Operational level: Lower management and administration

Figure 2: Conceptual model with detailed BIS processes and data, based on Von Solms and Von Solms [23].

Ownership of assets and risks, due to rotation of personnel, introduction of new tech-services without IT involvement, formal procurement processes (vendor vetting etc), mergers and acquisitions, rough and orphan assets become the new standard rather than an exception, let alone an adequate Configuration Management DataBase (CMDB) is presence. Proper administration of critical assets, their value, classification of the housed data, CIA ratings etc. is not in place nor centrally administered. Single pane of glass e.g. complete visibility over multiple point solutions that are related to risk, security, compliance. This forest of security tools causes decision latency[7] due to inefficient security operations that has limited interaction since the tools are owned, consumed, managed and measured by multiple actors e.g. auditors, IT managers, security staff, business users. This brings us to the main problem statement, which is:

"*Current emphasis of Zero Trust lies on architecture principles that are only understood by insiders. The current approaches and documents lack the alignment with risk management, existing frameworks and associated processes. Board and business involvement are not addressed and ownership of data, risks, security controls and processes is limited. And the main focus is on the change and not on the run and its value contributors".*

Considering the issues mentioned above there is a need to establish a more collaborative way of working among stakeholders when addressing the dynamics of the environment and the organization, gain a more qualitative and integral view based on facts related to tactical and operational data, to secure an increase in awareness at board level, to employ a certain level of reflection and self-learning to achieve continuous improvement and to use accepted best-practice frameworks produced and maintained by existing security communities and bodies. Therefore, the aim of this research is to answer the following main research question "How can we establish a method which utilizes best practices and collaboration for improving Zero Trust security maturity?"

In order to answer this main research question, we follow Wieringa [23] to distinguish Knowledge Questions (KQ) and Design Questions (DQ). Knowledge questions provide us with insights and learnings that together with Design Questions contribute in the construction of the design artifact (later referred to as Portal) since the artifact will be integrated in the exiting Managed Security Service Portal (MSSP) of ON2IT. This means that during the Design and development stages separate –requirement- design questions are formulated with the objective to design artifact requirements. The Design Science Research Framework of Johannesson and Perjons [24] is adopted and visualized in the figure below. This approaches follows earlier design and engineering efforts at the University of Antwerp and Radboud University [1,20] (Figure 3).

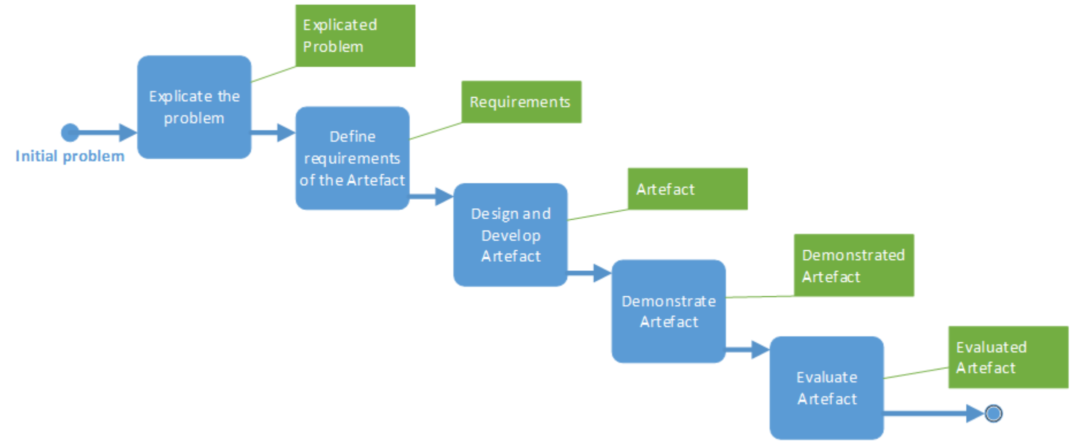


Figure 3: Overview of the framework for design science research [25].

In order to master the forementioned problems, we have formulated three major research questions:

I. What are Critical Success Factors for drafting and implementing ZTA?

II. What is an easy to consume a capability maturity -readiness- model and it's associated portal technology that

enables the adoption of ZTA and guides boards and management teams and facilitates collaboration and ownership?

III. How does the future empirical validation of the framework and the associated portal look like and provide

feedback to relevant stakeholders?

Before eliciting the research methodology, to gain answers and insights that contribute establishing the framework and technological portal we discuss the core concepts and historical evolution of Zero Trust.

What is Zero Trust?

Zero Trust is conceptually simple, yet elusive. In its dense form, the Zero Trust pitch is that it's an architecture that seeks to establish that "*inherent trust is removed from the network*" [25,26]. What is this 'inherent trust', then, and if there is such a thing, how do we remove it? Understanding this is key to understanding Zero Trust, and it requires a bit of knowledge about the technical innards of today's networking.

[7] The Standish Group: Decision latency theory states: "The value of the interval is greater than the quality of the decision." Therefore, to improve performance, organizations need to consider ways to speed-up their decisions.

The currently dominant form of networking is the TCP/IP protocol [27], which we'll just call 'IP' — the Internet Protocol. It is a layered protocol [28], and we'll take a look at the lower layers — because that's where this 'inherent trust' phenomenon arises. More specifically, it happens at the data link and network layers [29], where (at the data link level) data is broadcast across physical network using data framing, and where data packets (at the network level) are switched and routed (both slightly more selective mechanisms).

In a somewhat simplified history of computer networks, we started interconnecting computers directly. With A and B connected, anything sent by A is received by B. Scaling this up to interconnect multiple nodes, repeaters (aka bridges) were used to broadcast traffic from one host to several more. Switches are repeaters with an attitude. The classic 'LAN' came into being this way; a number of nodes directly able to communicate. And it's the 'directly' bit here that forms the implicit — or, we should say, inherent trust. Of course, as scale and (geographic) diversity of LANs grew (we're talking early '70s now), not only did LANs grow, but interconnecting LANs was the next step. Routers do this [30] and as more and more LANs got interconnected and the Internet broke out of its academic silo.

Speeding up a bit, the ensuing view of a friendly, comfortable 'inside' versus a hostile 'outside' has been prevalent for a long time. The classic interconnection model of the Internet was enriched by a classic Internet security model, that distinguished between 'trusted' (safe) and 'untrusted' (unsafe, the realm of the wily hacker [31]. True to classic field tactics, a defensive perimeter was concocted shielding trust from untrust. And thus, classic Internet security was born.

Speeding up even more, networks scaled up, gained a bit more depth, and loosened their physical ties. In physical networks, mechanisms to carry multiple separated broadcast networks over one single connections arose. This brought the realm of routing squarely into the LAN(s), as these became segmented, sliced up into interconnected smaller broadcast domains. As before, this gave rise to a (if you're built that way) more or less natural notion of perimeters inside the LAN.

Making one final leap, we zoom out a bit. Given the existence networks as a bunch of interconnected, internally transparent LANs and a general gut feeling of Internet xenophobia, Zero Trust rises to the challenge. Arguing that we've seen more or less free adversary agency on endpoints inside 'trusted' networks — end users being human and hence gullible, the technology they're using often fragile and poorly maintained and monitored - we should accept that systems on these 'trusted' can be breached and put to nefarious use too. And we should observe that, once a foothold inside is established, nothing stops an all-out rampage within the confines of the trusted network. As a witness, consider the flurry of utterly destructive 'ransomware' infestations, all caused by fragile, easily exploited inside systems with unfettered connectivity to vast hordes of other internal systems.

For this reason, Zero Trust breaks loose from the classic trust versus untrust train of thought. Everything is in a gray zone, and security incidents cannot be entirely prevented. The key properties a security should have is to limit security impact (containment) and to enable rapid response. This enables 'defence in depth' tactics, and seeks to take away the path to a single knockout blow.

Research and Development Methodology

DSR for the design and development of artifacts

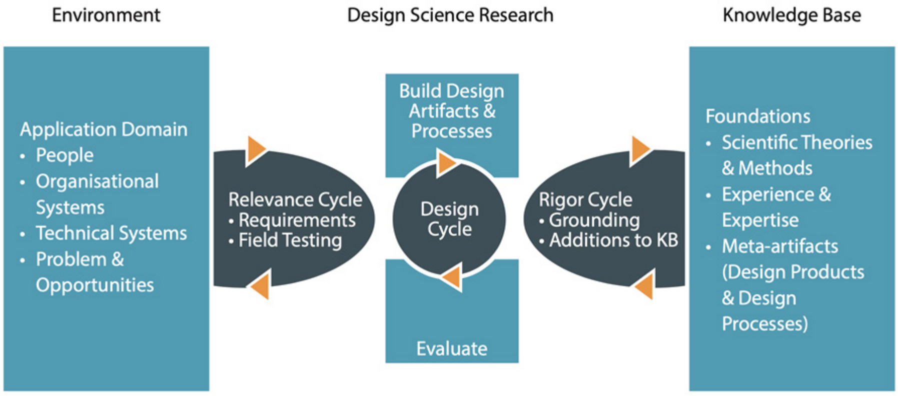


Figure 4: Hevner's Design Science Research Framework [33].

Design Science Research (DSR) has attracted increasing interest in the Information System research domain. March and Mith initiated important DSR work with their early paper on a two-dimensional framework for research on information technology [32]. Hevner et al. [33] produced a broad framework which is used worldwide to perform and publish DS work. This framework is visualized in see Figure 4 contrasts two research paradigms in information system research: behavior sciences and design sciences. Both domains are relevant for Information Security because the first is concerned with soft aspects such as the knowledge, attitudes and capabilities required to study and solve problems. The second is concerned with establishing and validating artifacts. To put it more precisely, Johannesson and Perjons distinguish between the design, development, presentation and evaluation of an artifact [25]. Wieringa distinguished many methods for examining numerous types of problems, e.g. design problems and knowledge problems [34]. In this Zero Trust project we used Hevner's work as a frame of reference for the entire DSR project and potential later validation by practitioners and we use Wieringa's approach to address the challenges and technical requirements we encounter during the current and future journey of portal development (Figure 4).

Doing DSR in a business environment

It would be too much to expect this research project to be performed in a perfectly situated environment and in an ideal sequence. Like any other longitudinal research new insights emerged from the problems we encountered during the execution of the research. The entire project, especially the design of the artifact, is performed in a practical business environment, so it is sometimes delayed by day-to-day problems. It is therefore required to re-engineer the entire research process and map it onto the Johannesson and Perjons guidelines for designing, presenting and validating artifacts [25].

According to earlier research projects, based on literature and expert research [1], we have started to examine literature on key Zero Trust topics and pitfalls. We have examined the following documents: Kindervag materials, NIST documentation, Forrester materials, Palo Alto Networks materials, Google documents on Beyound Corp, Scheerder (2012), Modderkolk (2018), Ward, R., & Beyer, B. (2014). BeyondCorp documentations, ISF (2018) Framework, Auditing Principles from the International Auditing Associations (IAA), CMMI Capability models, COBIT2019, ISO materials (Figure 5).

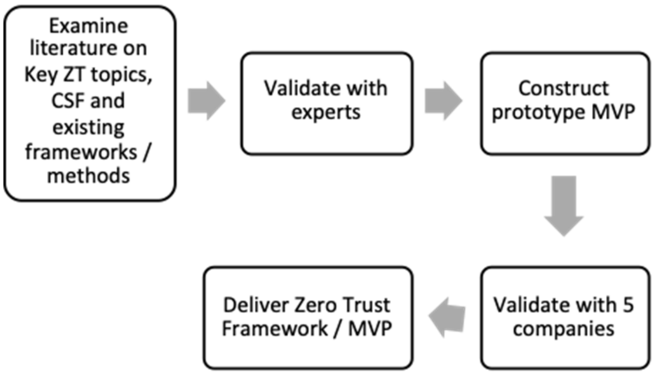

Examine literature on Key ZT topics, CSF and existing frameworks / methods
Validate with experts
Construct prototype MVP
Validate with 5 companies
Deliver Zero Trust Framework / MVP

Figure 5: Research approach to design and build the Zero Trust Framework and portal.

As an important step we have collectively with Antwerp Management School and ING Bank submitted the comments on the NIST Zero Trust Architecture Draft document (the NIST SP 800-207). During the month October and November of 2019 we have established a long list of 80 items and prioritized this to 26 items for future recommendations and used the commentary log (see table below) as source of shortcomings in the current approaches and required considerations.

Results

Based upon the above-mentioned insights from the literature and experiences we detail the following Critical Success Factors before and during the Zero Trust Journey of the implementation:

a) Engage and collaborate with relevant stakeholders on the value of Zero Trust for the business (e.g. proven control, reduce risks, decrease security spending, strengthen Trust position and the journey that lays in front of them. Since ZT is not simply switching the technical button. The role of the CISO is vital here. Hooper et al state; The role of the CISO is that of a strategic board adviser" [35].

b) Alignment with existing control framework and their scaling, metrics and taxonomy so it enables collaboration between second-line risk managers and third-line auditors have a common taxonomy, control objectives, Test of Design/ Effectiveness, metrics, goals and perceived outcomes.

c) Complete and accurate administration of critical assets (Data, Assets, Applications, Services) their economic value, CIA rating and their security requirements in a central repository (one source of truth). This single source of truth of the Security administration is a company's "license to operate". Especially in regulated companies. For some it is a Unique Selling Proposition [18].

d) Clear technology roadmap with Zero Trust based measures that have a clear definition of done and timelines for implementation and test of the Design and Effectiveness via existing Governance and reporting processes.

After listing these factors of influence for a successful implementation and maintenance of Zero Trust we have validated that with seven experts in the field and started constructing the artifact (initially in Excel) via an iterative process. The initial questionnaires that should capture the Readiness and Fitness on all organizational levels where constructed based upon four major improvements that should cover the shortcomings formulated in the problem statement, the improvements are;

I. Alignment with risk management & existing frameworks

II. Board and business involvement and explicit sign-off

III. Ownership for assets risks and measures

IV. Focus is on the change and on the run

When taking these improvements into consideration we come to the following definition of success factors that should be addressed via the framework and the portal technology:

"*Early involvement of Business owners and insight in their context, environment, capabilities and objectives, to understand the risk- appetite and prioritization. Explicate asset ownership and assess technology on their capabilities to utilize ZTA. Develop basic capabilities on monitoring and control progress and maintenance.*"

The On2IT Zero trust framework

This brings us to the three categories of the Framework with their associated rationale: (Table)

How the ON2IT Framework aligns

According to the forementioned shortcomings, extracted from the literature, in the current approaches the improved framework has the objective to act as a guide for boards and managers prior to starting a Zero Trust strategy and during the implementation. In this section we list the improvements;

i. A common language is used by making use of existing control framework as off level >3 for example ISF, NIST Cybersecurity Framework, NIST privacy Framework, PCI DSS or ISO27000 controls. We applied the CMMI based maturity levels on a 1 to 5 scale. Incl ISO15504 maturity criteria, based on audit terminology (ToD, ToI, ToE) that NOREA is using.

ii. Following category 1 (Know your environment and capabilities) you identify if business and IT alignment takes place, threats and trends are identified that influence the enterprise risk management (ERM) and assign appropriate ownership at board and managerial level (according to the COBIT EDM[8] model). The Framework enforces strict sign off for board members on preconditions that are required before you can implement Zero Trust. Organizations that use the COBIT5 or COBIT2019 processes and design principles can plot these to the EDM layers of Governance, Management and Operations. This brings the required common language.

iii. Each DAAS element requires ownership and CIA[9] annotation in a repository (e.g. CMDB) to ensure adequate asset qualification and even quantification so security measures can be assigned to these assets. We adhere to standard Business Impact Assessments (BIA) and Privacy Impact Assessment methods (PIA) by making use of a "Relevance score" on scale 0-100 composed of tags. 0 being a segment with low exposure and 100 with high exposure.

iv. By assessing the readiness of the organization in terms of processes and structures as well as the technological fitness to utilize Zero Trust there is transparency in the level of a successful ZT implementation, the "progress monitor" in the framework monitors the progress during and after the implementation.

How operational Zero Trust measures supports management and boards

In the Zero Trust architecture, controls aka measures are implemented to minimise the attack surface in depth, and to provide immediate visibility and, hence, swift and to-the-point incident response. What are some examples of these measures (based on the frame of reference in Table 1), and how can they be applied in a Zero Trust architecture? First, by identifying traffic flows relevant to a (closely coupled) application. In physical networks, takes the notion of segmentation a step further; the term 'microsegments' has been coined. By intention, such segments contain a (functional) application. By this additional segmentation, a 'microperimeter' is formed that can be leverage to exert control over, and visibility into, traffic to/from the contained (functional) application. A policygoverns the traffic flows, and a Zero Trust architecture not just prescribes defence in depth by isolation. We can be much more specific.

Policy regulating traffic to and from a Zero Trust segment

i. Is specific and narrow, satisfying the 'least access' principle: it allows what's functionally necessary, and *nothing more*;

ii. is, whenever possible, related to (functional) *user groups*

iii. enforces that traffic flows contain only the network applications;

iv. enforces content inspection (threat detection/mitigation) on;

v. *visibility* is ensured;

a. Logs are, whenever possible, related to individual users;

b. Presence and conformance of policy is operationally safeguarded;

c. Policy is orchestrated, if applicable, across multiple components in complex network paths;

d. Operational state and run-time characteristics (availability, capacity instrumentation) are structurally monitored.

[8] The COBIT5 for Information Security distinguishes Evaluation, Direct and Monitor for Governance of IT. This EDM model is distilled from the Von Solms brothers Direct Control Cycle for Information Security and widely used.

[9] The acronym CIA is used to determine the level of Confidentiality, Integrity and Availability and used to determine the Business Impact and thereby which control is needed to manage the risk within its appropriate boundaries of the appetite.

The very same concepts applied above to physical networks are used, unchanged, in virtual-, container-, cloud- or other software defined networks. In all cases, a way is found to create a logical point of 'visibility and control' that enables insertion and safeguarding of the appropriate controls.

Extending the Zero Trust architecture to end points is a step that is conceivable as well, considering the end point itself as a complex collective of potentially unwanted (malicious) processes to be safeguarded. At endpoint level, agency can be introduced to detect and mitigate malicious processes. When doing this, fine-grained endpoint behaviour extends the visibility beyond the network layer, and 'large data' analysis of (user) behaviour becomes viable, further deepening both visibility and defence in depth. Extracting the telemetry data -near- realtime from these technological measures is needed to feed this data back to tactical and strategical levels and promptly respond and telecommand back[10]. This relates to the increasing question; "how to inform the CEO in minutes after a breach?

Deliverables

Due to practical experiences we see that an important factor for Zero Trust success is to start with assessing the organizations readiness and technological fitness to adopt and execute Zero Trust. Therefore the "Framework" should initially consist of:

i. A Readiness assessment to determine how ready and fit you are as a company on the strategic level and managerial level.

ii. A Maturity assessment to determine your technological fitness level compared to objectives and potentially peers. This fitness level represents to what extend an organization is technical capable of utilizing the required Zero Trust measures and understand their limitations.

iii. A Progress Monitor to report to boards and regulators on a periodically basis and thereby involve them in the required decision making and avoid decision latency.

iv. An additional portal functionality built into the ON2IT Managed Security Services Platform Portal (also referred to as an artifact)

Future research

Assessing an organizations' posture with respect to Zero Trust viability requires evaluating these three levels, *and this ON2IT framework*. We propose four research areas:

i. Validation of the Zero Trust Readiness framework (pre- and post-implementation progress monitor);

ii. Assessing the presence and relevance of strategic capability attributes (strategic level);

iii. Assessing the presence and relevance of executive capability attributes (managerial Level);

iv. Assessing the presence and relevance of adequate technical capabilities (operational level).

These assessments determine the relevance, coverage, depth and actionability of the controls/objectives (at their respective level).

i. Zero Trust at the Strategic Level: Know Your Environment and Capabilities

At the Governance level, the following questions needs to be addressed:

a. To what extend are the defined questions in the readiness assessment relevant for board members?

b. To what extend do they appeal to boardroom level language and main dilemmas?

c. What topics are missing according to board members in the framework and portal?

d. What is the main target group to use the assessment or to take the assessment?

e. Who on this level is consuming the dashboard data and for what reasons?

ii. Zero Trust at the Managerial Level: Know Your Risk

At the Managerial level, the following questions need to be addressed:

a. To what extend are the defined questions in the readiness assessment relevant for management level? To gain better insight if the ZT approach appeals to business, security and IT management (as 3 different personas)

b. What topics are missing according to business, Security and IT management in the framework and portal?

c. Who on this level is consuming the dashboard data and for what reasons?

iii. Zero Trust at the Operational Level: Master Your Technology

At the Operational level, the following question needs to be addressed:

How do we add the necessary measures and leverage control and monitoring facilities thusly provided efficiently?

Classically, networks were built as islands of closely connected systems, separated by an explicit boundary. The notion of 'perimeter security' flows naturally from this blueprint. Inspection and enforcement typically takes place at 'north/south' boundaries.

[10] Telemetry is the collection of measurements or other data at remote or inaccessible points and their automatic transmission to receiving equipment for monitoring. The word is derived from Greek the roots tele, "remote", and metron, "measure". Systems that need external instructions and data to operate require the counterpart of telemetry, telecommand. Source: Wikipedia.

Citation: Yuri Bobbert, Jeroen Scheerder. Zero Trust Validation: From Practical Approaches to Theory. Sci J Research & Rev. 2(5): 2020. SJRR.MS.ID.000546. DOI: 10.33552/SJRR.2020.02.000546.

A slew of measures has arisen, allowing deep visibility into and control over network traffic by adding inspection- and enforcement capabilities at network boundaries: protocol validation, threat detection, application detection/enforcement, user-identification and RBAC-based network access policy, URL categorization and category-based access policy, and so on.

In virtual, container and cloud deployments there may not be a 'natural' boundary to segment he desired controls. Traffic might just as well be 'east/west', while still being subject (conceptually) to full policy enforcement.

Finding a way to enrich such deployments with the necessary controls then, is the key question.

i. How to embed full network security controls for 'east/west' traffic in virtual environments? With that control objective(s) are these controls aligned?

ii. How to add such controls in container environments? With that control objective(s) are these controls aligned?

iii. How to add such controls to cloud environments — brandX, brandY, ...? With that control objective(s) are these controls aligned?

iv. How to provision/orchestrate these control mechanisms and their policy? With that control objective(s) are these controls aligned?

(Table 2)

Table 2: Frame of reference for Technical Measures to utilize Zero Trust.

Measure Category	Technical measure for ZT utilization
Encryption	SSL Inbound Decryption
	SSL Outbound Decryption
	Encryption at rest
	Encryption in Transit
IAM / UserID	Centrally managed IAM (one source of truth)
	RBAC Based controls
	MFA
	Auditable (userID - logging)
(D)DOS	Volume Attacks (i.e. zone-protection)
	Targeted attacks (i.e. Policies)
Endpoint	Exploit Prevention
	Malware prevention
	Ransomware/Cryptolocker protection
	Central management
Traffic flows	Segments
	Restricted outbound access
	Restricted inbound access
	Application based/controlled
	Content-inspection
	URL based
	Behavioral analytics
Data	Credential Phishing prevention
	DLP controls are in place
	Data classification
	Data discovery
	Data/Applications have their own segment
Orchestrate/Automate	Rules of Engagement
	State validation
	Central policy management
Reporting	KRI, KPI

Table.

STRATEGIC 1. Know your environment and capabilities	The strategic level sets the direction of the company and sets the tone and soil for management and operations to execute the ZT strategy. Early boardroom involvement and their commitment is needed in order to define the relevant cyber actors, risks and critical value chains (including the assets) to the organization and how much appetite the company has. This set a common knowledge and understanding. Also, on the level of your own capabilities and talent your organization has and if it is equipped to win the cyber race.
MANAGERIAL 2. Know your risks	To execute the strategic directives and make management decisions you need to know which ones first. Therefor management needs to have basic processes and structures in place (reporting, roles and accountabilities) to instruct operations to build or run security tools and to get feedback on the utilization performance. Business management needs to understand their critical business processes (value chains) and IT management needs to understand together with business which logical segment supports these processes and of which data, assets, applications and services this segment comprises. *Definition of a segment:* Segment being "A logical part of the environment which consist of collaborating data, assets, applications and services that represent a certain value, business dependency and exposed to certain risks"
OPERATIONS 3. Know your technology	In order to implement Zero Trust security measures in these segments the organization needs to determine if the existing technology is equipped to do this. Or if the organization needs to acquire additional technologies or implement additional processes or services. An assessment on the operational fitness and the alignment with upper DAAS processes is done. In general, as well as per segment.

The relevance of these measures derives from the need for both *visibility* and control. Taking charge, taking control, first and foremost requires insight. As an example, to be able to detect and mitigate malware activity, a thorough view of network activity is required. Yet part of that activity might be hidden from sight because a confidential communication channel is used, using cryptographic techniques. For the purposes of control, subverting that (by intention) confidential communication channel is desirable.

At the meta-level, presence (or: detection of potential absence) of controls is important. Network security is not monolithic, it pertains to a complex chain of related items across diverse components. In addition to having (potential) visibility and control, verifiable implementation across the chain is also a precondition.

(Figure)

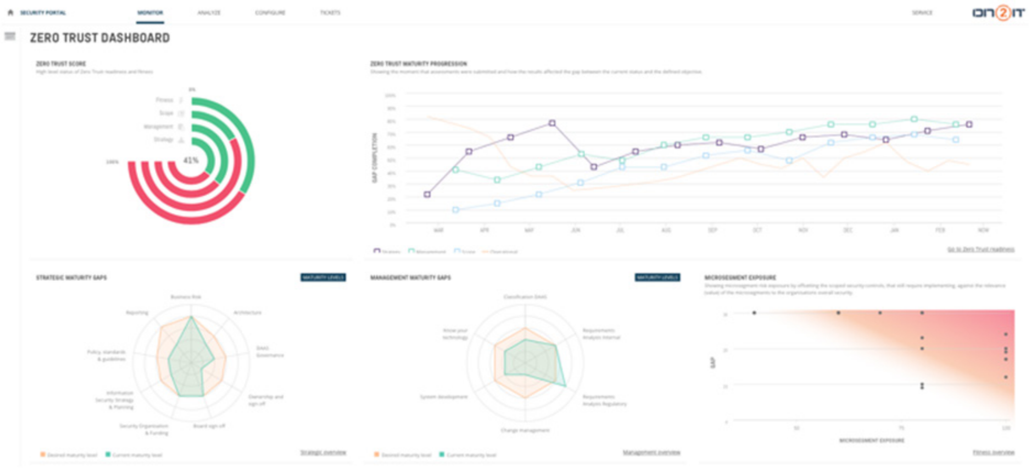


Figure.

To execute this empirical validation with practitioners, sessions are held and facilitated via Group Support System [1]. The use of GSS in validating frameworks, technological artefacts and models is described in multiple papers [1,18,36,37]. The use of GSS will also be used to validate the portal technology developed by ON2IT to support the Zero Trust Framework. In the screenshots below examples of the established artefact are displayed [38].

Conclusion

The ON2IT Zero Trust Framework explicitly recognizes all major shortcomings in the current approaches such as the lack of board and business involvement and explicit sign-off to assure commitment. The ON2IT framework structures the ownership and responsibility for asset risks and controls. These assets and control are clearly defined in the 'classic' Zero Trust concepts of segments and transaction flows. By forcing the Zero Trust concept of segmentation 'up' into the boardroom strategic risk level, the connection between risk and the required controls becomes much more tangible and manageable than in existing frameworks. Mainly due to the fact that names are attached to assets.

A key design goal of the ON2IT Zero Trust Framework is to formalize the involvement of organization asset owners from a business perspective, yielding in more insightful interpretations of concepts such as *recovery time objectives and risk appetite.*

The framework transparently addresses the readiness requirements at the three separate organizational levels of cybersecurity and provides insight and control across these levels with a common language and metrics for relevant measurements. Because the effectiveness of operational controls is assessed in relation to the Zero Trust segments defined at the upper levels, the alignment of risk and technology can be designed and measured with greater precision and cost-effectiveness. The 'relevance score' of every individual segment, a concept integrally embedded in our methodology and Zero Trust orchestration and automation portal, drives the required controls and the required dynamic feedback on their effectiveness. This is a real time process. This simply cannot be a static process otherwise you cannot inform your "upper" levels with adequate information. Further research and development for both the framework as well as the portal technology is needed in order to improve organizations security maturity, the security and risk administration, decrease risks and lower the operational cost of information security to focus on what really matters.

Conflict of Interest

No conflict of interest.

Acknowledgement

None.

References

1. Y Bobbert (2017) Defining a research method for engineering a Business Information Security artefact. Proceedings of the Enterprise Engineering Working Conference (EEWC) Forum, Antwerp, Belgium
2. (2005) ITGI, Information Risks Who's Business, are they?. IT Governance Institute, United States
3. M Siponen, R Willison (2009) Information Security management standards: problems and solutions. Information & Management 46(5): 267-270.
4. D Kluge, S Sambasivam, (2008) Formal Information Security Standards in German Medium Enterprises. Conisar, Phoenix.
5. Puhakainen P, SM (2010) Improving employees' compliance through information systems security training; an action research study MIS Quarterly 34(4): 757-78.
6. M Workman, W Bommer, D (2008) Straub Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior 24(6): 2799-2816.
7. B Lebek, J Uffen, M Neumann, B Hohler, M Breitner (2014) Information security awareness and behavior: a theory-based literature review. Management Research Review 12(37): 1049-1092.
8. W Yaokumah, S Brown (2014) An Empirical Examination of the relationship between Information Security / Business strategic alignment and Information Security Governance Journal of Business Systems. Governance and Ethics 2(9): 50-65.
9. W Flores, E Antonsen, M Ekstedt (2014) Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. Computers & security 43: 90-110.
10. J Pfeffer, R Sutton (2001) The Knowing-Doing Gap: How Smart Companies Turn Knowledge into Action no. Harvard Business School Press.

a. Lawson A (2005) World without Boundaries Butler Review Journal Article.

11. M Modderkolk (2018) Zero Trust Maturity Matters: Modeling Cyber Security Focus Areas, Utrecht: University of Utrecht.
12. B Jagasian (2020) Another Buzzword Demystified: Zero-Trust Architecture. ISACA Journal.
13. KJ (2010) Build Security Into Your Network's DNA:The Zero Trust Network Archit Security.
14. J Van Niekerk, R Von Solms (2010) Information security culture; A management perspective. Elsevier, pp. 476-486.
15. T Papelard (2017) Critical Succes Factors for effective Business Information Security, Antwerpen: Antwerp Management School.
16. R Von Solms, B Von Solms (2006) Information Security Governance; A model based on the Direct-Control Cycle. Computers and Security. Elsevier Computers and Security 25(6): 408-412.
17. Y Bobbert (2018) Improving the Maturity of Business Information Security. Nijmegen: Radboud University.
18. Volchkov (2013) How to Measure Security from a Governance Perspective. ISACA Journal, p. 5.
19. YON Bobbert (2020) Lock Chain technology as one source of truth for Cyber, Information Security and Privacy. Computing Conference, London.
20. Kankanhalli T, Hock-Hai, C Bernard, W Kwok-Kee (2003) An integrative study of information systems security effectiveness. International Journal of Information Management 23, Department of Information Systems, School of Computing. National University of Singapore, pp. 139-154.
21. L Sanchez, A Santos-Olmo, E Fernandez-Medina, M Piattine (2010) Security Culture in Small and Medium Size Enterprises. Communications in Computer and Information Science 110: 315-324.
22. Solms von R, Solms von B (2006) Information Security Governance_ A model based on the Direct-Control Cycle. Computers and Security Science Direct 25(6): 408-412.
23. R Wieringa (2014) Design Science Methodology: For Information System and Software Engineering. Berlin: Springer.
24. P Johannesson, E Perjons (2014) An introduction to Design Science. Springer, Stockholm University, Sweden.
25. H Stuart (2019) Zero trust architecture design principles.
26. R Stevens (1993) TCP/IP illustrated: the protocols. Addison-Wesley Longman Publishing Co., 75 Arlington Street, Suite 300 Boston MA, United States.
27. RFC1122 (1989) Requirements for Internet Hosts - Communication Layers. Internet Engineering Task Force.
28. R Perlman (1999) Interconnections: bridges, routers, switches, and internetworking protocols. Addison-Wesley Longman Publishing Co, 75 Arlington Street, Suite 300 Boston, MA, USA.
29. RFC1812 RFC 1812 (1995) Requirements for IP Version 4 Routers. Network Working Group.
30. C Stoll (1988) Stalking the Wiley hacker. Communication of the ACM 31(5).
31. S March, G Smith (1995) Design and natural science research on information technology. Decis Support Syst 15: 251-266.
32. S Hevner, J March, Park, S Ram (2004) Design Science Research in Information Systems. Management Information Systems Quarterly 28(1): 75-105.
33. R Wieringa (2009) Design science as nested problem solving. Proceedings of the 4th international conference on design science research in information systems and technology, New York.

34. V Hooper, J McKissack (2016) The Emerging role of the CISO. Business Horizons, 56. Kelly School of Business, Indiana University, Elsevier, pp. 585-591.

35. Y Bobbert, J Mulder A (2010) Research Journey into Maturing the Business Information Security of Mid-Market Organizations. International Journal on IT/Business Alignment and Governance, United States 1(4): 18-39.

36. Y Bobbert, J (2013) Mulder Group Support Systems Research in the Field of Business Information Security; a Practitioners View. in 46th Hawaii International Conference on System Science, Hawaii US.

37. E Alqurashi, G Wills, L Gilbert A (2013) Viable System Model for Information Security Governance: Establishing a Baseline of the Current Information Security Operations System. 28th Security and Privacy Protection in Information Processing Systems (SEC), pp. 245-256.

38. G De Vreede, RO Briggs, R Van Duin, B Enserink (2000) Athletics in Electronic Brainstorming; Asynchronous Electronic Brainstorming in Very Large Groups. Proceedings of the 33rd Hawaii International Conference on System Sciences.