It has been 10 years since John Kindervag, then with Forrester Research, first laid out the information systems security concept called the zero trust model. In the decade since, few organizations could boldly claim that their information technology environments were safe from hazards and threats emanating from the inside and outside. Organizations’ core business processes are more tightly integrated with information systems. Adoption of various IT outsourcing arrangements and cloud computing applications appears to be on the rise. Cybersecurity breaches have grown in sophistication and the degree of damage they create. A zero trust approach to information security appears to offer tight control over all systems by not trusting any request to access any information resource.

How do information systems leaders make the move to a zero trust model? The frequently cited 2010 Forrester Research white paper, No More Chewy Centers: Introducing the Zero Trust Model of Information Security, offers several immediate steps organizations can take to begin their transformation to a zero trust model. The first is:

Change how you think about trust. This involves changing your thinking about trust models and becoming aware of the misuse of the word “trust” in relation to networking and security. Once attuned to how inappropriate trust is in the infosec realm, you can socialize the Zero Trust concept throughout the organization.1

The white paper also discusses network analysis and visibility products, explaining that their use:

…[S]ends a message to potential malicious insiders. Once [network analysis and visibility] NAV is deployed, tell people that you’re going to be watching what they do. This will change behaviors. If individuals know that security is monitoring their actions, they will be less tempted to do things that are questionable.2

This will change behaviors. It is important to question what unintended consequences can be caused by a zero trust environment. Is it possible it may negatively impact employee attitudes and lead...
to changes in enterprise culture? Various intra-organizational trust frameworks suggest that if left unchecked, zero trust principles have the potential to sow the seeds of distrust among employees and between employees and management.

Relying on concepts from organizational culture and trust research, it is worthwhile to explore how attitudes underlying a zero trust approach can spread beyond the information system environment and impact organizational culture.

Zero Trust Architecture

Developed in the days following the global recession of 2008-2009, zero trust architecture is a strategy aimed at preventing "successful data breaches by eliminating the concept of trust from an organization's network architecture."3 Examined as a secure network strategy by US federal government agencies more than a decade earlier, zero trust's conceptual ancestor, "de-perimeterization," was first promoted in 1994.4 The basic premise of zero trust is to "assume that every part of your network is potentially hostile, as if it were directly on the Internet, and treat access requests accordingly."5 The absence of trust in users—the requesters—no matter who they are, where they are or what they ask to access is the foundation on which the zero trust model is built. This skepticism is reinforced in Zero Trust Networks: Building Secure Systems in Untrusted Networks: In this model, nothing is taken for granted, and every single access request—whether it be made by a client in a coffee shop or a server in the data center—is rigorously checked and proven to be authorized.6

Threats to a Zero Trust Environment

Various information technology professionals acknowledge that network security effectiveness under the perimeter approach continues to be challenged by the number of users and types of devices requesting access to network resources.7,8,9,10 To mitigate these risk areas, the zero trust approach reverses the older emphasis on blind or implied trust of users. Zero trust requires a "very pessimistic view on security where every machine, user, and server should be untrusted until proven otherwise."11

On the surface, this sounds like a dream: a well-oiled system operating with surgical precision and efficiency. But a zero trust environment is not without its dangers. There are several weaknesses, including:12

- Outsiders stealing user credentials
- Risk posed by insiders
- Access to stored network traffic and metadata
- Absence of human intervention in managing permissions (e.g., overreliance on artificial intelligence [AI] or robotic process automation [RPA] to handle network security)

From a financial perspective, return on investment (ROI) for systems supporting a zero trust architecture might be a high hurdle to clear.13

Little has been written about zero trust's potential negative impact on an organization's culture of trust. But it is important to address concerns about the trickle-down impact of not trusting employees.

Trust

What does it mean to trust? Trust can be explained as:

The willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party.14

An earlier definition of trust is "an expectancy held by an individual or a group that the word, promise, verbal or written statement of another individual or group can be relied upon."15 Some trust scholars acknowledge that there is no universal trust definition, but they identify four essential parts of trust: uncertainty, vulnerability, expectations and willingness.16 It is important to note how each definition of trust contains overlapping elements.
Three Trust Framework
In *Trust and Betrayal in the Workplace*, a trust framework was created based on three elements: contract, communication and competence. Contractual trust is a “mutual understanding that the people in the relationship will do what they say they will do.” Communication trust is gained when parties “share information, tell the truth, admit mistakes, maintain confidentiality, give and receive constructive feedback, and speak with good purpose.” When parties recognize others’ “skills and abilities, allowing people to make decisions, involving others and seeking their input, and helping people learn skills,” competence trust is created.18 *Becoming a Trustworthy Leader: Psychology and Practice* evaluates the quality of trust relationships according to four factors: reliability, openness, competence and compassion.19 Trust between people is enhanced when the trustor believes the trustee demonstrates dependability, sincerity, capability and proficiency, and empathy.

Another commonly cited trust framework states that trust is earned according to three attributes projected by the trustee: ability, benevolence and integrity (ABI).20 Can the trustee make things happen (ability)? Is the trustee’s kindness genuine (benevolence)? Does the trustee follow a “set of principles” on which both find common ground? All three attributes (ABI) contribute to the act of trusting another (e.g., a co-worker, a manager or the organization): “it is possible for a perceived lack of any of the three factors to undermine trust.”

Zero Trust and the Culture of Enterprise Trust
Enterprise culture is not just the sum of its individual employees’ beliefs about culture. It acquires an existence of its own, linked to—but sometimes independent of—each employee’s collection of ideas about the proper way to analyze, choose and act. Within this enterprise culture, shared beliefs and values influence how employees perceive, behave and understand the organization’s norms for proper behavior, setting the “context for everything an enterprise does.”21

“Key here is the phenomenon of trust. The idea in this is if you first locate whom you cannot trust, then you know what the salient risks are.”22 When the implicit message communicated by a zero trust approach is that everyone is a risk and no one is to be trusted, employees can feel the psychological contract with their employer has been broken. A psychological contract can be described as the informal corporate culture mechanisms that “motivate workers to fulfill commitments made to employers when workers are confident that employers will reciprocate and fulfill their end of the bargain.”23 Organizations put systems in place to ensure that employees are trustworthy. “The efforts to prevent abuse of trust are gigantic, relentless and expensive; and inevitably their results are always less than perfect.”24 Although the effectiveness of monitoring and auditing for bad behavior or abuse of trust in the workplace has its limits, abandoning trust on a wholesale basis is not the solution either.

When an organization adopts a zero trust environment, it is important for the organization to consider how the decision will be perceived by employees and how it will alter the trust relationship between employees and the organization. Organizations should consider which of the three aspects of trust (ABI)—is central to the trustee’s earning trust from the trustor. “Clearly, if all three factors were high, the employee would trust, but how low can some of the three factors be before the employee would not trust the manager?”25 It is worth thinking about past experiences where trustees have lost the trust of a trustor and which of the ABI aspects was lowest or did not exist.
"The risk of depending on others—is generally regarded as the first condition for trust" and "trust serves as a trustor's expectation of a trustee's trustworthiness." Yet in a zero trust environment, management explicitly and implicitly takes the stance that the trustee (the employee) is neither dependable nor trustworthy. In a study of IT security culture in small and medium-size enterprises in Australia, "local organisational culture will affect the information security culture." Consider how the information security culture impacts the culture of an organization.

An article in the Harvard Business Review discusses the appearance of a virus that is contaminating workplaces: oversight systems. "If it is even partly true that a lack of trust makes employees untrustworthy, it does not bode well for the future of virtuality in organizations."  

Trust has seven essential values:
1. Trust is not blind.
2. Trust needs boundaries.
3. Trust demands learning.
4. Trust is tough.
5. Trust needs bonding.
6. Trust needs touch.
7. Trust requires leaders.

In a work environment where people are naive, unbounded, inflexible, soft, impersonal, isolated and rudderless, the absence of trust as promoted by a zero trust approach has the potential to penetrate the culture of information systems and spread unchecked negative behaviors into the organization's culture.

Conclusion
When there are appropriate levels of trust within an organization, employees believe its decision-making processes and decisions are just and that they are fairly treated and experience just interpersonal interactions at work. Higher levels of organizational trust are supported by a strong corporate culture. Intra-organizational trust is particularly important in diverse work environments, "the development of mutual trust provides one mechanism for enabling employees to work together more effectively."

In observing earning trust during periods of uncertainty, researchers note that perceptions of trust vary among various groups of employees. The amount of time an employee has worked for an organization and the degree of seniority plays a role in the amount of trust employees place in their employer. Newer employees and those who have reached higher levels of seniority tend to place more trust in the organization's decisions and actions during periods of instability. In addition, "local subcultures"—small clusters of employees with shared interactions and unique characteristics and viewpoints—can react differently to rapid changes. This complicates the corporate culture of trust.

In a 1995 Harvard Business Review article, one author wrote, "Virtuality requires trust to make it work: Technology on its own is not enough." Twenty-five years before the novel coronavirus turned many workers into stay-at-home employees and workplaces into virtual organizations, the author of this prescient quote recognized the threats to enterprise culture posed by a lack of trust.

Author's Note
The author thanks Dr. Beverly Hogue and Dr. Nicole Livengood of the Marietta College (Ohio, USA) Faculty Publishing Group, who offered helpful feedback on drafts of this article.

Endnotes
2 Ibid.
5 Goerlich, J.; W. Nather; T. Pham; Zero Trust: Going Beyond the Perimeter, Cisco DUO, 2019, https://duo.com/resources/ebooks/zero-trust-going-beyond-the-perimeter
7 Ibid.
8 DelBene, K.; M. Medin; R. Murray; The Road to Zero Trust (Security), Defense Innovation Board, USA, 9 July 2019, https://media.defense.gov/2019/Jul/09/2002155219/-1/-1/0/DIB_THE_ROAD_TO_ZERO_TRUST_(SECURITY) _07.08.2019.PDF
10 Op cit Kindervag
11 Op cit Gero
12 Op cit Rose
18 Ibid.
19 Mishra, A.; K. Mishra; Becoming a Trustworthy Leader: Psychology and Practice, Routledge, USA, 2012
20 Op cit Mayer et al.
26 Op cit Li
29 Ibid.
31 Op cit, Society for Human Resource Management
32 Op cit, Mayer et al.
34 Op cit Handy