Zero Trust Business Objectives

August 02, 2022

Director, Community Ecosystem Engagement - Cybersecurity

Michael is a world-leading IT industry analyst. He has led North American and global initiatives focused on developing insights and strategies that connect technology solutions with business needs, combining data, knowledge, analysis and advanced content delivery to define options for IT and buy-side businesses.

Submitted by Michael O'Neil on 2, Aug 2022
Zero Trust Business Objectives

Zero trust thought leadership group members: Geeta Kapoor (MSC Direct), Noah Davis (Trane Technologies), Leon Ravenna (KAR Global), Barney Baldwin (ex-MUFG, Columbia), Chase Cunningham (Ericom), Eve Maler (ForgeRock), Sean Frazier (Okta).

Zero trust (ZT) supports business objectives for three personas. For the senior leadership team, ZT enables the achievement of business outcomes. For the CIO, ZT supports better control over IT costs and capacity. For the CISO, ZT supports the development of security capabilities that align with both vulnerabilities/threats and evolving business needs. By articulating and connecting these goals, businesses are able to ensure that ZT initiatives deliver meaningful payback.

Executive summary

It’s tempting to state that because every aspect of a digital business relies on secure technology, zero trust will have an impact across all business objectives. But our research finds that ZT business objectives are better understood in terms of depth rather than breadth.

Zero trust has a meaningful, beneficial impact on organizational capacity to address key executive concerns: an enterprise's ability to roll out new capabilities quickly, support major corporate transactions, and build stakeholder confidence. ZT supports CIO objectives by reducing complexity and streamlining processes used to deploy needed business systems and can even provide a means for reducing shadow IT. CISOs need to address senior executive and CIO imperatives and have a third set of goals – focusing defense on critical corporate intellectual property (IP) assets rather than the network perimeter, maturing key practices (particularly concerning identity), and helping the security function to evolve from reactive firefighter to collaborative, forward-looking business partner.

Zero trust business objectives in three "stories"

Businesses have only a few top-level imperatives pursued by the senior leadership team at the direction of the board of directors: increased revenue, decreased cost, improved profitability (a function of the first two goals), reduced risk, and/or improved shareholder value (which may result from one or more of the other objectives). Most security initiatives focus on risk reduction. More broadly, technology leaders are often expected to enhance the organization's ability to control costs. Outside of software companies and tech companies, it is rare that IT or security contributes directly to revenue growth or increased shareholder value.

From this perspective, zero trust represents an unusual opportunity for security and IT. The primary function of ZT is risk reduction, and (as covered in other sections of this series)[1] zero trust can contribute to cost savings, at least within the security function itself. With increased reliance on digital business, however, zero trust also supports activities that drive revenue while delivering proactive defense against cyberthreats that can harm corporate reputation.

After analysis of our discussions with the cybersecurity thought leadership group, Stratascale divided zero trust business objectives into three "stories" – one focused on senior leadership team (SLT) imperatives, one on the CIO's perspective, and one on how ZT advances business goals that are important to CISOs themselves.

The SLT story

- External research on ZT has shown that "your business will be more agile, your development processes would be more secure…which means faster to market,

your employees will be more satisfied, and you will have less security spend."

- "Having an effective zero trust strategy can help you adopt newer [business-critical] technologies. So, though the [business unit] manages these connected [IoT] devices, the business can [deliver better outcomes] because it is able to integrate new technology capabilities."
- When we onboard a new M&A acquisition, "We start with 'extreme zero trust,' where [the new acquisition systems, staff, and suppliers] don't touch our network until we're comfortable…by default, from an M&A standpoint, the stance we take is that you are segregated until we need to bring you in. And then we have the controls in place [to manage integration securely]."
- "We deal with the largest banks in the country, and there's a lot of what I call 'backhand legislation' – you need to go do this thing and then make sure all your vendors are doing it too."
- "We talk about corrupted data. You *know* data is getting corrupted. You can have attacks, of course, where data is changed, including cases where you don't even know the attack occurred. But incidents are a contributor to data rot in ways you may not fully understand. And it contributes to brand risk. So [it matters to] anybody who has any kind of known brand…it affects everybody and everything."

These five quotes encapsulate extensive discussions exploring ways that ZT supports core business objectives in the digital era. As one contributor observed, in many environments, "mission-critical describes a business outcome" – a patient's health, the uninterrupted flow of a production line, or access to an ATM machine or credit data.

While delivering these outcomes may be more difficult (or, in some cases, impossible) without technologies that are more quickly and safely deployed in organizations that have implemented ZT frameworks, ZT itself is not an objective for most non-IT executives. But as the contributor noted, organizations that are slow to deploy new IT-enabled capabilities will fall behind those that are more efficient or that offer unique services. In organizations that don't protect against intrusion, "in some cases, a security breach will prevent a function from occurring" – and in those cases, the supplier could be sued by a patient, customer, or other stakeholders. "So, there's both exposure in terms of the ability to support core functions *and* from the perspective of needing to demonstrate that all reasonable steps and precautions have been taken to reduce or remove post-incident liability."

The first quote above summarizes ZT benefits against this backdrop; the contributor who cited the research added, “Find me any business that doesn't want to be more agile, put out more stuff, have happier employees, and reduce spend!”

The second quote digs into the impact of ZT in enabling the integration of new technologies that support innovation, such as IoT devices in hospitals or manufacturing environments. The contributing CISO added that a ZT framework helps streamline future rollouts by standardizing the processes and approvals for new products requiring network access: “If the security architecture team [has already vetted and approved an advanced product], you can just buy the equipment, and it's already on the network, right? There's zero validation required because it's already been through that process.”

The third and fourth quotes highlight areas where security is integral to corporate financial interactions. The first of these deals with using “extreme” zero trust to build an integration path for new acquisitions that provides access to needed information without compromising network security, while the other quote makes an interesting point regarding “backhand legislation,” in which financial institutions pass on responsibility for supply chain security as part of specific transactions or relationships. Meeting such requirements is a very difficult hurdle for firms that treat each new requirement as a one-off. It is far more straightforward for companies to apply zero trust principles to all requests and interactions – they can quickly attest to safe interactions with vendors because this type of security is inherent in the ZT approach.

The final quote in this sequence talks about perception and reality concerning corrupted data. The reality is that absent careful and comprehensive inspection, incidents may occur that degrade data – sometimes without the knowledge of the business. Even incidents that occur without becoming public knowledge – not only an undiscovered attack but also, for example, unsanctioned access to records that are moved or changed by an insider using improperly configured credentials – can erode internal trust in data and external trust in the brand, devaluing important corporate assets.

The line between CISO and SLT responsibilities is blurring. One contributor observed that “the three topics that are gearing up to be [top corporate priorities] are M&A, supply chain, and how people will implement privacy in the US.” Each of these is a C-level or board-level responsibility, requiring active and effective involvement from

the CISO. Increasingly, the executive team and board will expect the CISO to consider multiple “bottom lines” – What is critical to the business? From a security perspective, what is critical to enable the business to function optimally?

The CIO story

- “Deferring cost adds exponentially to complexity over time.”
- “We think ZT would eliminate a lot of shadow IT, which is a big problem in [our industry/many industries]…I think [line-of-business (LOB executives)] feel authorized to purchase any IT solution without engaging IT. And if we have all the components of zero trust in place, it would prevent them from buying anything off the shelf that may not be secure.”
- “Removing the delays in provisioning new solutions…every time a new piece of equipment comes to the loading dock [including both IT and IoT-type systems that attach to the corporate environment], we have to do a security architecture review on it to identify what will it touch, what [sensitive/regulated] information will it have, network segmentation – all those requirements. If we are buying things and implementing them in this established structure and we put this new widget in a right zone, if you will, it follows policies that have already been established. And I think that's going to reduce a lot of the onboarding delays that we see from an application or a hardware perspective.”
- “Another thing [ZT] helps you do, thinking about the core business and thinking about the data, is it actually helps you reduce complexity. We've played whac-a-mole with our protections because we don't really know where our data is or how important our data is: we just added security protections everywhere and we buy every product under the sun and we have a stack of 25 things we're just layering on and we're hoping that we're going to get security through complexity. But you don't get security with complexity. You get the exact opposite. The only people who benefit from complexity are attackers.”

CIOs are continuously balancing tension between corporate demands for greater capability and concurrent spend management (or reduction), as well as competing priorities within the IT department. Most of the IT budget is allocated to maintaining, upgrading, or replacing existing assets or supporting new capabilities. CIOs have little scope for investment in net-new technology or approaches. However, they are still expected to act as a source of innovation for digitally dependent business

functions while also allocating resources to risk reduction.

It is easy to see why CIOs would elect to defer investments if they don’t address urgent priorities. But as the contributor quoted at the top of the list above noted, cost deferral does not lead to cost savings. It can be argued that delayed spending actually leads to increased costs because resources that are unavailable where/as needed impose a “tax” in the form of time spent waiting for access.

It is very clear that deferred investments – especially with respect to zero trust, which rationalizes controls and products to establish a consistent framework enabling proactive risk management and avoiding reactive measures that do not create value for the IT operation as a whole – will add to the complexity because postponing needed investments results in sprawl, by leading to deployment (or impeding removal) of diverse, potentially duplicative technologies, each of which increases maintenance and skills-related overhead.

Delaying IT investments also encourages business units to make technology investments on their own, connecting unsanctioned devices or applications to corporate networks and resources. This poses a security risk and is also a major financial headache: analysts estimate that somewhere between 20% to 50% of all corporate IT spending goes to shadow IT. Zero trust helps the CIO control shadow IT by streamlining how new devices, applications, and other assets gain access to the corporate environment. This both allows the IT department to react more quickly to business requests and provides visibility into unauthorized IT resources as they attempt to connect to the corporate network.

The final quote above speaks to another topic that is of concern to CIOs: complexity. CIOs are painfully aware that complexity adds cost and increases risk. They likely know or suspect that complexity works in favor of external attackers, not the cyber defenders in their own ranks. Zero trust is designed to streamline operations, controls, products, and even vendors – each of which offers a clear advantage to the CIO as they balance conflicting imperatives.

The CISO story

- “From an identity perspective, our processes right now are not mature. Once we implement zero trust, what function somebody has and what access they're going to get will become very predictable, and that can be automated. From an

end-user perspective, the experience will be much better."

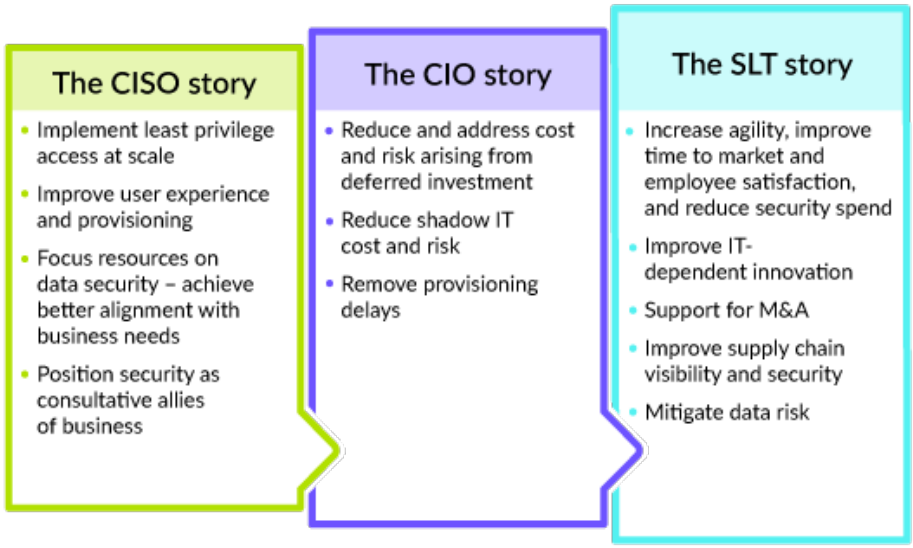
- "Zero trust can help businesses focus on what they do for a living. And again, it's conjunction with cloud services. It's conjunction with mobile endpoints and all these different things. What an organization owns from an IT perspective is less and less important – what's important is the ability to focus on their core business – which, from an IT perspective, means data. Zero trust is all about focus on the data and not so much on all the stuff that lives around it."
- "There is the classic mismatch – impedance mismatch, if you will. Businesspeople are saying, 'But I need to make this much, I need to launch this campaign!' and then you've got [security] people appearing to be boat anchors. But I think information security has become a lot more consultative, and that's a good thing – [security is now] calling out where the mismatches are and seeing if you can find something that satisfies both [business and security] requirements."

Much of the CISO's story is written in the sections dedicated to the SLT and CIO – CISOs need to support objectives in both areas while also contributing to the management of cyber risk and other corporate risks, if or as required.[2] On top of this, CISOs strive to obtain needed and scarce resources (especially skilled staff) and to remain abreast of the constant stream of cyberthreats.

The quotes above expand on core CISO ZT issues. The first speaks to the benefits anticipated from providing users with a consistent experience and rapid access to resources; this contributor also predicted that zero trust would speed up provisioning as well since the process for vetting new products and providing them with resource access will also become faster and more predictable.

The second quote speaks to a recurring theme in research conducted for *The Technical Manager's Guide to Zero Trust,* which Stratascale is delivering as a companion series to this Executive Guide material. Repeatedly, internal Stratascale SMEs discussing different ZT pillars returned to the subject of data security, which was universally seen as the objective of zero trust rather than one of six component focus areas. As the quote shows, focusing on the data aligns security with core business objectives. Expanding on this, members of the zero trust thought leadership group view ZT as a way to not just treat "data security" as a point in time statement or objective but as something that can enable the development of a posture that the business can maintain through changing circumstances and across time.

The final quote observes a change in the relationship between business and security professionals. Historically, there has been tension (arising primarily from mismatched incentives) between business leaders demanding support for financial or time-bound goals and security professionals tasked with preventing exposure to cyberthreats. The contributor believes that security is evolving to deliver more guidance (and reduce time lost to conflict) by identifying areas where business objectives are at odds with security mandates and working with their product or customer-focused peers to find ways of responding to the pressures felt by both CISOs and business leaders.



Source: Stratascale 2022

Working with this content

CISOs looking to integrate this perspective on zero trust within executive-level strategy discussions can use the following challenges/constraints and takeaways to

inform their approach.

Key challenges/constraints on ZT as a means of supporting business objectives

- Zero trust effectively supports SLT goals if/where the CISO is an important part of the discussion. If the CISO (as an example) learns about a new acquisition from news reports, they will be hampered in their ability to provide value to M&A evaluations and integration or divestiture strategy.
- Zero trust shines a light on (and limits access for) shadow IT activities. Business unit leaders who rely on non-sanctioned systems – especially those with a track record of success despite limited formal IT support – may oppose measures, including ZT, that hamper their operational latitude.
- The first step in data security is data visibility. Automated discovery is a "must have"; manual processes cannot keep pace with data sprawl. Organizationally, corporate silos that impede access to data (especially sensitive data) will limit ZT efficacy.

Takeaways from "Business Objectives"

- At a time where "digital business" *is* business, better and more proactive management of technical risk can convey significant competitive advantage: increased agility, improved time to market, increased employee satisfaction, and ultimately, reduced expenditures on redundant security technologies that add to complexity rather than capability.
- ZT can and should be a CIO priority, as it provides a means of reducing risk, streamlining processes, and establishing a degree of shadow IT visibility and management.
- ZT delivers on core CISO business objectives, improving user experience, focusing resources on the highest-priority data assets, and helping the security function to move beyond its reputation as an impediment to rapid progress, repositioning security leaders as consultative partners delivering effective support to business operations.

This is the fourth of eight source documents included in Stratascale's "An Executive Guide to Zero Trust" research series. We will also publish a capstone report connecting these eight pieces, a six-part companion series ("The Technical

Manager's Guide to Zero Trust"), and several compilations and ancillary documents and tools.

[1] See, in particular, Key Considerations in Zero Trust Rollouts.

[2] For more insight into cyber risk and cyberthreat management, please see Cybersecurity Strategy for the Looming Regulatory Quagmire.

Readers interested in specific executive-level perspectives on zero trust may wish to explore the other publications in this series: