Zero Trust Sponsorship and Commitment

July 19, 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 19, Jul 2022

Zero Trust Sponsorship and Commitment

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

To date, zero trust (ZT) champions have been security rather than business leaders. There are signs that this is changing – and that the change will bring about better outcomes.

Executive summary

To date, ZT champions have tended to be CISOs rather than business leaders. Increasingly, though, non-technology executives – particularly those with risk, compliance, and privacy responsibilities – are sponsoring ZT within their organizations. This is an important change, as senior leadership team (SLT) backing is essential to organization-wide ZT success. Security leaders looking to build executive support should express the ZT strategy regarding business outcomes without relying on technical language. Organizations must recognize that compliance, risk management, and privacy are business issues, not security problems. Security leaders who position ZT in terms of its ability to reduce friction and enable agility are most likely to win executive endorsement for ZT.

Building effective zero trust sponsorship

Zero trust sponsorship has been shifting. CISOs have been the primary sponsors for ZT initiatives in most organizations and continue to drive ZT within most companies today. But there is a groundswell of ZT leadership from outside the security function – and the zero trust thought leadership group identifies this business sponsorship as an essential step in positioning ZT as a business rather than a security concept.

ZT in the executive suite

- “It [the position of the internal ZT champion] has finally started to change. A year ago, almost everything [ZT initiative] was coming from security people. But in the last, say, five months, [ZT leadership has] started to come from boards, CEOs, business leaders, those types of people. And I think that's a really good thing.”
- “Zero trust is a security initiative, but a business decision.”
- “Zero trust has got to be a business objective, and not just a framework or a security platform.”
- “I think there's a lack of knowledge [concerning zero trust within the executive suite]… I think people have heard this term, and they get the overarching objective. But how it would actually get implemented and where it gets implemented is still a little nebulous. So, executives are hesitant to say ‘yes, let's move forward and let's create a project called zero trust.’”
- Is there an executive sponsor for [ZT]? “‘Kind of.’ [Executives] agree with the objective, but they don't know what that means.”
- “If we had to sell zero trust [to the board of directors], we would have to take the technical components of it out and show ZT fits into the overall program.”

Should security leaders raise the topic of zero trust for discussion with senior executives? Contributors shared a wide range of perspectives. Some members of the thought leadership group opted to emphasize the benefits of executive buy-in to ZT activities. Others highlighted current knowledge gaps, noting that while executives have some interest in the concept, they have next to no understanding/awareness of what zero trust entails from a time, cost, or activity perspective.

Substantial executive backing for ZT is relatively recent. Multiple contributors cited the Biden Administration Executive Order 14028 (12 May 2021) as a key event triggering executive interest in ZT. Other contributors avoid discussing “zero trust” with SLT and board of director members altogether, noting that “they're already trained on what NIST means. So, where does zero trust fall within those frameworks? Which gaps is it filling?” There is also, these experts believe, exposure associated with ZT as a concept, as leadership may ask, “if we are [investing in] being more proactive, how can we reduce budget or resources on the reactive side?”

Contributors on all sides of this issue emphasized the benefit of committing to an enterprise-wide ZT strategy. One contributor pointed out, “Organizations that [implement] zero trust in pockets will not realize its benefits. The narrative will turn

to, ‘zero trust isn’t working right.’” Firms that commit to a cohesive end-to-end strategy will realize benefits, while those that dabble will conclude that ZT isn’t worth the investment.

First steps to executive relevance

- “I have seen [business executive champions for ZT] be successful. And in a lot of cases, that person is going to be someone who cares about risk and who cares about privacy.”
- “Cyber security is a risk function shared between CISO and the CRO [Chief Risk Officer].”
- “[ZT] increasingly is driven out of a compliance obligation. And sometimes, security doesn't sit in that organization. I've been working to try and make [ZT] a business conversation, talking about ‘privacy’ and ‘digital transformation’ and all those other things that I have to put into scare quotes.”

In cases where ZT *has* obtained business backing, support originates with executives who have risk, privacy, or compliance obligations. In these scenarios, security leaders can act as advisors and enablers, supporting objectives that concern the business as a whole. As one contributor said, ZT “can't just come from IT…[CISOs can say] you need to fix your business processes. But this means making [security generally, ZT specifically] a priority from a risk perspective,” rather than strictly as an IT objective.

Real-world constraints to business sponsorship

If Zero Trust aligns so well with executive priorities, why do CISOs often struggle to obtain executive sponsorship? Contributors point to the disconnect between security objectives and business objectives.

- “The business is about reducing friction. The security folks are all about closing gaps and accepting no risk. And they don't mind if a user has to go through 20 hoops to do something because that's not what they care about. They care about the protection. They don't necessarily care about the experience.”

- “IT typically doesn’t generate revenue. We are pure overhead. So the best way we can [contribute] is to make it easy for the business to do the things that they need to do. I know zero trust does that. And I know that *talking* about zero trust doesn’t do that!”
- “[Motivating] board-level action at the business unit level is extremely challenging because business units have been working in more traditional environments and making a lot of money – in some cases, with not very much IT support.” Business unit executives who have succeeded without IT’s support are very likely to push back on change requests from IT.
- “Traditionally, the buying point for security technology has been IT, but now, business leads are more apt to reach out to suppliers directly. They don’t want to involve IT ‘because the new system is for the customers, not employees.’”

These observations point to gaps in both perception and reality. In fact, not every CISO will eschew user convenience to increase the number of controls. Still, the fact that this perception exists suggests that this characterization is at least *sometimes* accurate. And it is certainly true that some business units succeed with sub-optimal IT support, and quite likely true that leaders of these units will push back on increased constraints from or budget allocations for a security/IT function that has been less than completely responsive to their needs.

Putting the emotions reflected in the statements aside, there is scope for better alignment of controls with real threats. One expert noted, “we end up adding all the friction to our actual users and very little friction to our attackers. If we think about things from a user experience perspective, we want to add less friction to our users and more friction for our attackers – and that very much aligns with zero trust philosophies.” CISOs who can draw this distinction improve their prospects of building credibility with skeptics in the business.

Internecine strife

Even within the IT function, misaligned incentives can lead to tension. The CISO’s interests are best served by “pipes closed” – strict limits on access and data ingress and egress. The CIO, on the other hand, is more directly aligned with business colleagues and will consider “pipes wide open” – ubiquitous, flexible employee access to assets across and outside the corporate environment and customer and supplier access to internal systems – as a preferred end state.

One contributor was asked, “Where does the board sit on this? Are they in favor of making things as fluid as possible for the user community, are they in favor of making things as locked down as you'd like to see as a CISO, or are they somewhere in between?” The response made it clear that neither the CIO nor CISO agenda shapes board priorities: “it's always going to be somewhere in between,” the expert stated. “It's all about managing an acceptable level of risk.”

The case for executive support

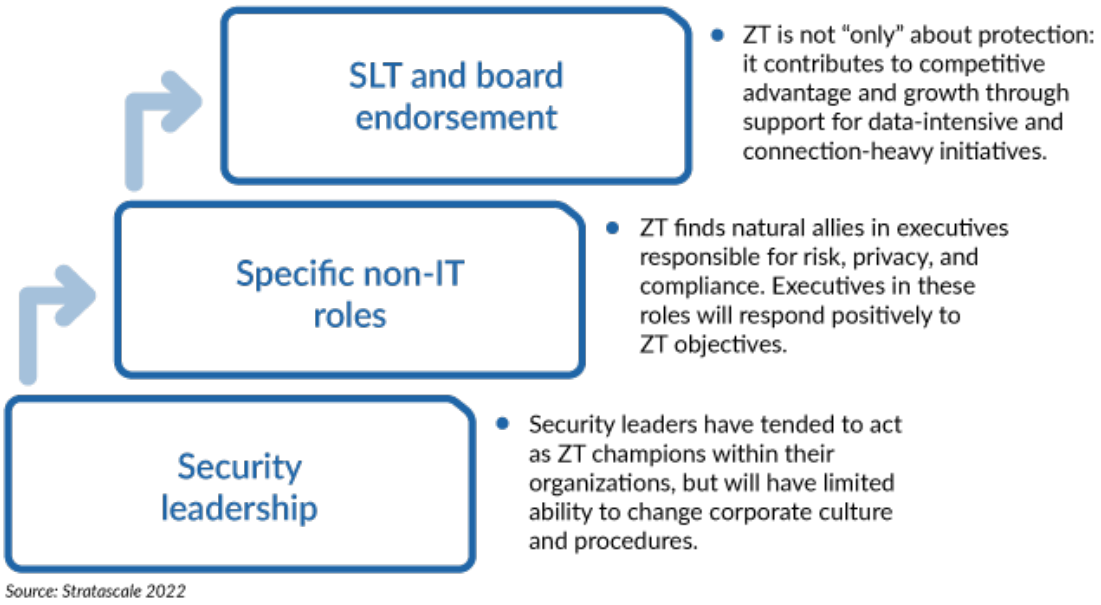
- “PCI should never, ever be perceived as being owned by the security department. That is a business feature. There are elements of that, like vulnerability scanning and multifactor authentication, that IT security can help with, but [compliance is] way more successful in companies who treat PCI as a business objective, who treat GDPR as a legal and business objective.”
- “I think it's really important to understand that regulatory compliance is being driven from a business perspective. That’s when we see security leaders be way more effective in their implementation of zero trust—[when they position ZT as] how you achieve compliance, how you protect that IP [intellectual property], instead of just something you want to do to have better security.”
- Talking about ZT as a security concept to C-level execs is “a career-limiting move.” “Whereas, if I talk about simplification and enablement and frictionless security, that’s speaking to them on their terms.”

The most effective path to building a case for executive support for ZT is to focus on business objectives and avoid deep, technical discussions of key technologies and implementation imperatives.

The first quote above observes (correctly) that compliance is not ultimately the responsibility of the security leader – that it is “owned” by legal and business executives. The final quote marks an intriguing alternative path to building executive endorsement of ZT: emphasizing security objectives that are considered important by stakeholders throughout the organization. This contributor stated that “the two terms I use a lot are ‘frictionless security’ and ‘the flexible future.’”

The key, this CISO believes, is to “end up making [ZT] *their* [the executives’] idea,” through repetition of terms that resonate. “I know I've won,” this SME stated, “when my leaders or other people start repeating my phrases back to me and think it's their idea.” In this way, the CISO obtains executive endorsement for the (relabeled)

ZT journey, building top-down support for the evolving deployment by aligning tightly with business imperatives. “Fundamentally,” the CISO observed, “what you’re trying to get to is frictionless security. That helps enable your business – and it enables [the business] to be flexible to meet the needs of customers.”



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 to building executive endorsement for a ZT strategy

- It is difficult to present a holistic vision for ZT to a non-technical senior executive audience.
    - “Zero trust is a very technical concept. So how do you raise it up to a level where you explain it, but in terms of business value, saying that you're going to streamline provisioning? Giving an example of what ZT will do is good, but its impact doesn’t seem as great as the cost is going to be.”
    - “I haven’t broached the whole concept of zero trust with the board or the audit committee. We’ve had to simplify our asks and our progress for that level. We’ve been using things like the NIST framework to show our maturity, to show our risk and show our road map.” [Introducing a new vision for security would create friction in these discussions.]
- Privacy, compliance, and risk are business issues and should be treated as such. Organizations that see these as “security concerns” are setting the CISO up for failure: they will not build the enterprise-wide commitment to pervasive, adaptive protection of IP and corporate environments that is a prerequisite for success in the digital economy. The inverse holds as well: security leaders who attempt to drive ZT without executive endorsement will struggle to build momentum within the business.
    - Security can guide the business and identify potential vulnerabilities in new systems. But if security strategy and practice are driven purely by the security organization, “it just doesn't work. Like in the overused adage ‘it takes a village,’ everyone in an organization needs to be part of the security conversation – and if [that conversation] is driven by the business with the support of security, it’s way more successful than security trying to push everyone else along.”
    - “Zero trust needs to take shape from a business perspective. If you have a security leader who's latched on to [ZT] as a way to improve their security program, they may struggle. They may try to evangelize and promote zero trust, but may fall short […] in terms of cost, in terms of culture, in terms of executive alignment.”

Takeaways from “Sponsorship and Commitment”

- The entire organization benefits from effective zero trust collaboration. “Make security a partner because access is about monetization just as much as it is about protection.”

- CISOs should look for ways to “position [ZT] as a business competitive advantage, with the CEO treating like they would treat an ERP deployment, which is only successful if you drive it from the top down at the executive level. If [the organization] treats zero trust the same way, as a business-aligned enablement, then you're going to be way more successful.”
- Build a holistic ZT framework, but focus on building agreement on business objectives, using terms that resonate with the SLT and board; align incremental actions that address business goals with the ZT plan.

This is the second 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, ancillary documents, and tools. Readers interested in specific executive-level perspectives on zero trust may wish to explore the other publications in this series: