Global Knowledge Brief

Cybersecurity

Part 3: Establishing a New Zero-trust Boundary

The Institute of
Internal Auditors

About the Experts

Adam Kohnke

Adam Kohnke, based in Madison Wis., is the information security manager of chemical manufacturing company Charter Next Generation.

Julio Tirado

Julio Tirado is the executive vice president, director of Internal Audit and Compliance, at SpiritBank based in Tulsa, Okla.

It should be a baseline requirement for every organization to have processes and controls in place to keep their networks secure. However, as technology has advanced and networks have grown larger and almost unfathomably complex, the standard for what constitutes a secure network has changed. One of the most important changes lies with the transition from a location-centric security model to a more data-centric one. We call this model “zero trust.”

What Is Zero Trust?

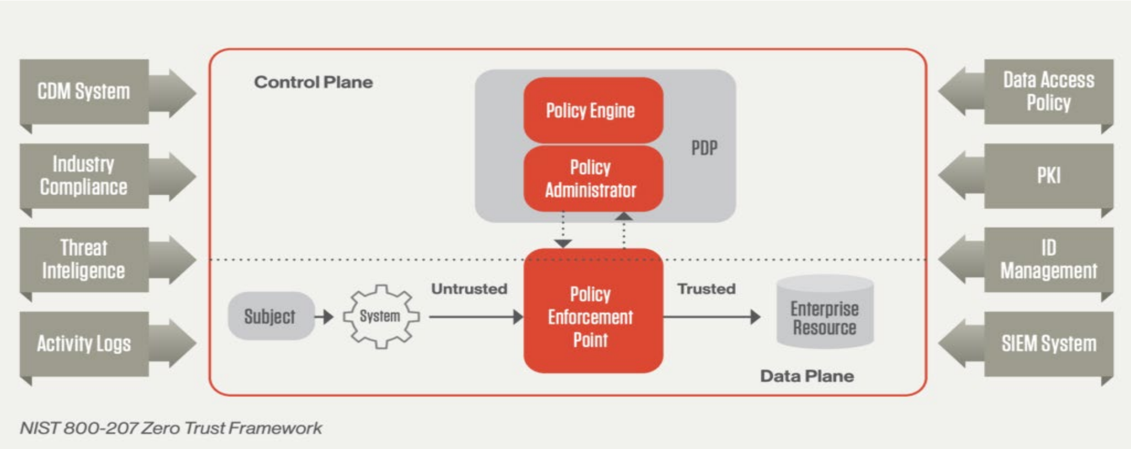
Generally, a zero-trust security framework requires all users that operate within a network — both inside and outside the organization itself — to be authenticated before accessing applications and data, and then continually validated regularly. As the name implies, “trust,” or more specifically “trust but verify,” plays no part in this system and access to anything enterprise-related must be continually justified and assessed based on the policies of the organization.

Traditionally, cyber models were built based on the location of the network, but in a zero-trust system, what constitutes a “network” is less strictly defined, as an organizational network can be local, based in a cloud, or a hybrid of the two. Especially following the COVID-19 pandemic, which ushered in a new era of remote work, hybrid or entirely cloud-based systems have become the norm, and cybersecurity frameworks have had to evolve to account for it.

There are several formal zero-trust frameworks in existence, including:

- Standard 800-207 from the National Institute of Standards and Technology (NIST). This is the framework mandated for use by U.S. federal agencies since 2021 (See Figure 1).
- Google BeyondCorp.
- Microsoft Zero Trust Strategy.
- Zero Trust Maturity Model from the Cybersecurity and Infrastructure Security Agency (CISA).

Figure 1



NIST 800-207 Zero Trust Framework

Source: Zero Trust Networks | NIST

While they all have their unique attributes, they do each share the same baseline principles, namely:

- Continuously verify access across all resources.
- Minimize the impact area in the event of an external or internal breach.
- Use behavioral data to gather context from the IT infrastructure.

While a transition to such a system can seem substantial, it is important to note that it is not meant to be a substitution for current systems. “Zero trust doesn’t seek to fully replace current network protection models or even infrastructure changes,” says Adam Kohnke, information security manager at chemical manufacturing company Charter Next Generation, “but rather to augment them for enhanced network protection. It’s meant to be an extension because traditional systems such as firewalls, web proxies, and boundary isolation mechanisms were not working.”

According to IBM, the average cost of a single data breach in 2024 was $4.88 million. Additionally, the average life cycle of a breach was a full 292 days from identification to containment. Clearly, traditional network protection has not been sufficient and requires significant attention.

The Internal Audit Role

While details can vary, internal auditors can have a variety of responsibilities associated with the implementation and maintenance of a zero-trust system. To illustrate, here are areas where an internal audit assessment may have the most value.

Defining Protected Surfaces

Traditionally, a cybersecurity system concentrated its efforts on defining what the security parameters were around an enterprise network. Firewalls and VPN systems are designed around this concept, keeping sensitive data and vulnerable information as far as possible from the network perimeter. In a zero-trust system, however, instead of parameters, the focus is on groupings of data, applications, assets, and services (DAAS), known collectively as “protect surfaces.”

Assuring these surfaces are appropriately identified must be central to a comprehensive internal audit assessment, says

According to Julio Tirado, executive vice president, director of Internal Audit and Compliance at SpiritBank, “The assessment should focus on inspecting the organization’s data classification policies to determine if systems and data are classified appropriately, and if the protection policies in place for each are appropriate.”

Protected services are not just limited to data, either, Tirado says. Physical assets that have a role in accessing sensitive data also must have processes and procedures in place to ensure they are inventoried and periodically assessed.

> The assessment should focus on inspecting the organization’s data classification policies to determine if systems and data are classified appropriately, and if the protection policies in place for each are appropriate.
>
> – **Julio Tirado, SpiritBank**

Verifying Map Transaction Flows

Once there is assurance that protection surfaces are identified, the next step in the assessment process is to ensure that there is stakeholder understanding of how all these DAAS systems interact with each other. IT teams should have detailed documentation diagrams dedicated to mapping out the complex web of ports, network traffic baselines, and protocols that collectively outline how these systems access each other and where their use can lead.

Although in most organizations the internal audit function may not have the sufficient knowledge or experience to verify the accuracy of these diagrams on their own, Kohnke says internal audit can work with the stakeholders or trusted third party to ensure validation tests are conducted to ensure what is depicted is sufficient. “What is important,” he says, “is that relevant DAAS is accounted for within each diagram and if sufficient details are present … and whether initial security policies defined in the previous steps have been modified or require additional controls.”

Verifying Creation and Ongoing Improvement of Zero-trust Policies

Zero-trust policies should be detailed for each protective surface and should answer critical questions such as:

- Who should be permitted to access enterprise DAAS systems?
- What applications will be allowed to access enterprise DAAS systems?
- When should access to enterprise DAAS systems occur or be occurring?
- Where are enterprise DAAS systems located?
- Why does the enterprise DAAS systems need to be accessed?
- How should access to enterprise DAAS systems be granted?

To assess the relevance and validity of created zero-trust policies, continuous interaction with IT stakeholders is critical as the enterprise network continues to expand and evolve. “Zero trust is not a destination,” says Tirado, “so security policy and DAAS protection requirements should evolve as the process unfolds.”

The goal, says Tirado, should be to have an ever-improving policy dedicated to addressing every type of traffic that could enter, exit, and traverse a network. “There should not be anything within a network where the source or purpose can’t be identified,” he says. “The internal auditor in their assessment needs to determine if reviews are conducted, if they are conducted to a sufficient extent, and if the policies in place accurately address what they find.”

Zero-trust Architecture Monitoring

As the previous examples indicate, ongoing monitoring is critical to the success of a zero-trust framework. Unlike a traditional system, where monitoring would focus on security parameters, the monitoring systems of a zero-trust system will center around users, devices, and services. “Monitoring should be carried out on your networks to measure performance, identify all devices attached to your network, and detect rogue devices and malicious activity,” says the National Cyber Security Centre in its zero-trust guidance. This is especially true if you're hosting on-premise services, but as it has become more common, mobile device management should be considered in equal measure.

“Companies like mine will deploy mobile device management software that will provide a measure of control for that particular device, as long as the user accepts it,” says Tirado. “It will monitor activity, help restrict dangerous sites, restrict certain software that can be installed on the device, and provide a control for deploying updates to that particular system.”

> Monitoring should be carried out on your networks to measure performance, identify all devices attached to your network, and detect rogue devices and malicious activity.
>
> – **National Cyber Security Centre**

Additionally, monitoring should include not just the actual use of systems but also how long they are being used. As stated by the National Cyber Security Centre, “User behavior, like normal working hours or normal working location, is [an] important metric to monitor.”

There are various monitoring systems available designed to meet the specific needs of the network in question, but generally, these systems will transfer collected data to a central location where it can then be analyzed. This information, over time, will establish a "baseline" for what constitutes normal behavior regarding variables such as transaction volume, asset communications, and user activity.

Through their assessments, internal auditors can ensure that regular reviews of this data are conducted — and that management takes appropriate ownership of this task — and that their findings create a baseline that accurately reflects the reality of the network.

"For internal auditors, a lot of it comes down to governance," Tirado says. "Management must be informed of the role they play in securing the system, because the system isn't going to stand long on its own. Changes to security policies are determined by what the baseline establishes as 'normal' and 'abnormal.' Management reviews set that baseline."

Establishing a Baseline

Like many elements of cybersecurity, or indeed risk management, there is no "one-size-fits-all" model, and as such how the internal audit function contributes to it will vary significantly. "It depends on the resources," Tirado says. "It depends on the size of the organization. It depends on the mandate of the internal audit team."

A good place to establish a baseline, he says, is to map out an assurance-providing process not unlike any other audit system. "As an example, think of Sarbanes Oxley," he offers. "Every public company must map out the internal controls related to financial statements, developing this matrix. And as a part of that mapping, you're going to create testing procedures through a given period — like a given year. You would take the same approach with zero trust, breaking down assurance to pieces throughout the year, taking into account the size of the company, resources, etc."

The common throughline among all cases, however, is the obligation of internal audit to continually champion the implementation and ongoing improvement of a zero-trust system. There are a variety of resources on the market that help with this task, based on the element the zero-trust model is focusing on. For example, regarding ransomware risks, Tirado uses InfraGard, a free information-sharing tool developed through a partnership with the FBI and members of the private sector. In just a few minutes at the beginning of each day, Tirado can use the tool to get up to date regarding the latest ransomware attacks and data breaches both inside and outside his industry. "The scale of these attacks begs for an approach beyond a perimeter-based security model," he explains. "Keeping stakeholders informed of what the risk environment looks like and what's at stake is internal audit's number one priority."

Additionally, it is important to note that this is not a transition that needs to happen all at once. "Even in partial form, a zero-trust model has immense value," says Tirado. "At the end of the day, a zero-trust model boils down to a spreadsheet column of controls. Maybe it's 20, maybe it's just 10 or 12. Well, that's better than five."

Examples of simple controls to consider in the early stages of a zero-trust model include:

- Data Encryption.
- Security Awareness Training.
- Incident Response Plans.
- Endpoint Detection and Response systems.
- Mico-segmentation.
- Compliance Monitoring.
- Behavioral Analytic and User Entity Behavior Analytics.

The Foundation Is Already There

Despite the core philosophical change in the network, internal auditors should realize once zero trust is understood, the responsibilities of the function itself should not be wholly different from what was expected of them before. Zero-trust implementation itself requires no architecture or infrastructure changes outside of the possible adoption of certain commercial tools, so neither do the systems that provide assurance for it.

Indeed, the key tenets of any audit work include identification, communication, and assurance, and each of those responsibilities remain intact. With a steady hand, adherence to the Global Internal Audit Standards, and a willingness to learn, the transition to a zero-trust network architecture is nothing an organization should fear.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 255,000 global members and has awarded more than 200,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes only. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as peer-informed thought leadership. It is not formal IIA Guidance. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Global Knowledge Briefs are intended to address topics that are timely and relevant to a global internal audit audience, and each topic covered is vetted by members of The IIA's volunteer North American Content Advisory Committee. Subject-matter experts are primarily identified and selected from The IIA's list of Global Guidance Contributors.

To apply to be added to the Global Guidance Contributors list, email Standards@theiia.org. To suggest topics for future Global Knowledge Briefs, email Content@theiia.org.

Copyright

Copyright © 2024 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact Copyright@theiia.org.

December 2024

The Institute of
Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101