GLOBAL PERSPECTIVES & INSIGHTS

Cybersecurity

PART 1: Cyber Threats in an AI-enhanced World

PART 2: Ensuring Cyber Resiliency

PART 3: Establishing a New Zero-trust Boundary

The Institute of Internal Auditors

PART 1

Cyber Threats in an AI-enhanced World

About the Experts

Antonio Cacciapuoti, CIA

Antonio Cacciapuoti is the head of internal audit at Eurizon Capital S.A. Luxembourg, the asset management company of Intesa Sanpaolo Group.

Bradley Niedzielski, CPA

Bradley Niedzielski is an audit and assurance partner and the Finance Transformation and GenAI Leader at Deloitte & Touche LLP, where he serves public and private firms in the financial services industry.

During the last year, advances in artificial intelligence (AI) have left organizations scrambling to keep up and to understand the opportunities and threats these technologies represent. As part of that effort, companies need to consider the growing danger that AI can pose to their security efforts, especially given businesses' near-total reliance on online information and transactions. Bad actors have quickly turned to AI-enhanced tools to improve their ability to break through companies' cyber defenses. This brief examines how cyber threats have changed in an AI-driven world and how internal audit can help companies develop new cybersecurity approaches in response.

An Evolution in Cybercrime

While strong cyber defenses have always been critical, bad actors are now using AI to sharpen and broaden their ability to overcome organizations' defenses. "AI is not a new type of cyberattack, it is an evolution," says Antonio Cacciapuoti, head of internal audit at Eurizon Capital S.A. Luxembourg. AI is used in ways that are more advanced than traditional cyberattacks in terms of speed, scale, complexity, and adaptability. In addition, "like a virus, it builds up resistance over time, making it more dangerous," he says.

AI is being used in attacks that range from narrowly focused to broadly destructive. For example, while many in the business world now regularly use AI-generated documents for emails or reports, bad actors also use AI-created documents for criminal purposes, says Bradley Niedzielski, audit and assurance partner at Deloitte in New York.

On another front, phishing attacks aim to break through security barriers and gain access to valuable data. While phishing isn't new, the FBI warns of AI-driven phishing attacks "characterized by their ability to craft convincing messages tailored to specific recipients and containing proper grammar and spelling, increasing the likelihood of successful deception and data theft."

Automated spear phishing, for example, is personalized for one person or a group and aimed at stealing sensitive information or gaining access to a system. "AI can analyze social media, communication patterns, and available data about a target, then craft messages more likely to trick recipients into revealing sensitive information or click malicious links," Cacciapuoti explains. At the same time, while it might have been possible to trust a video or call in the past based on knowledge of a person's voice or features, with deepfakes (simulated videos of an individual) and voice hacking, which replicates a person's voice, it's possible to deceive and manipulate specific targets.

These aren't the only AI-related threats organizations face. AI-powered malware can adapt and change its behavior based on the target environment, making it harder for the traditional security system to detect, according to Cacciapuoti. "It can easily escape basic detection and use polymorphic techniques to change its code and even analyze defensive measures to avoid them," he says. Even more important, it can introduce poisoned data into an AI machine learning model used in a fraud detection system, leading the AI to make inaccurate predictions and overlook some fraud indicators.

Using smart data exfiltration, AI can analyze stolen data and intellectual property in real time and prioritize which information is the most valuable for exfiltration. It can then encrypt that information and demand a ransom to release it, he says. AI-driven attacks also can compromise the credentials that authenticate valid users, enabling them to move across the system.

The risks of AI-driven cyberattacks are important because the stakes are so high. The leak or misuse of sensitive information could harm an organization's competitive standing or subject it to penalties for failing to comply with data privacy regulations. Any breach could drive customers and business partners to lose trust in the organization. Ransomware and malware attacks can disrupt operations and shut down critical systems.

Many uses would have been unimaginable not that long ago, but they are playing out in real time today. For example, an employee at a multinational firm in Hong Kong unwittingly paid $25 million to fraudsters after being convinced to do so by a deepfake simulation of the company's chief financial officer in a video call, according to CNN.

Elsewhere, The Drive reports that a Ferrari executive received a phone call from a deepfake claiming to be the company CEO. The attempt was foiled when the suspicious executive asked a question only the CEO could answer. In a case cited by Greylock Partners, a North Korean spy used a fake identity to get hired by a cybersecurity firm, then immediately installed malware on its corporate devices.

The Best Defense

Fortunately, AI also can help organizations thwart bad actors. "To stop AI, you have to use AI," Cacciapuoti says. Organizations need to adopt more sophisticated AI-powered cybersecurity measures to keep up with evolving threats. "If you don't have deep knowledge of the technology that criminals are using, how can you stop them?" he asks. Organizations should familiarize themselves with the tools and strategies cybercriminals are using and understand the many ways they can help enhance cybersecurity.

"The Need for AI-powered Cybersecurity to Tackle AI-driven Attacks," from ISACA, identifies numerous ways advanced technologies can help prevent attacks:

Ways to Prevent Attacks

- Analyzing vast datasets to determine how organizational resources are used, spot exposed areas, create an asset inventory, and identify network traffic trends and user activities/behaviors.
- Detecting anomalies, including "unusual logins, access requests from a new geographic location or IP address, new user access, change of permissions on files and other resources, extracting or deletion of large volumes of files, and an exponential increase in traffic."
- Using AI to proactively lock out, log off, or otherwise block suspected bad actors and alert system administrators to their activity.
- Continuously monitoring systems to enable speedy responses.
- Using predictive analysis to anticipate potential security threats and take steps to prevent them.
- Detecting and preventing zero-day threats, or new and unseen vulnerabilities.
- Cutting down on the number of false positive potential threats.
- Automating security assessments to speed responses and minimize human errors.
- Scaling to adapt to new developments and environments to provide ongoing protection.

Organizations can leverage AI to aggregate, analyze, and correlate data from multiple sources to create deeper insights, Cacciapuoti says. They also can use natural language processing (NLP) to analyze large textual data. For example, when internal auditors are asked to analyze contracts, NLP can extract important textual data for the system to analyze.

Addressing AI Considerations

Because an organization can never address 100% of the risk, Niedzielski recommends beginning by strategically assessing the threats across different areas of the business. That will include identifying potential AI fraud vectors and evaluating the likelihood they will be attacked and the potential magnitude and impact. The next step, he says, is to determine the effectiveness of existing controls.

As part of this effort, Niedzielski recommends using GenAI's emerging capabilities, such as advanced reasoning and pattern recognition, to recognize common tactics such as AI-generated phishing attempts and deepfakes. Some companies use protocols and technologies to verify whether a call has been made from an internal or external number.

"These advanced technologies can help minimize the associated risk," he says. In some cases, however, such as making an immediate determination on whether a caller or meeting participant is a deepfake, employees may have to rely on gut feelings or be ready to question why a CEO is calling and asking for a funds transfer, for example. In these situations, employees should be encouraged to trust their instincts and call the person back on their company number or, if the purported caller is in the same office, simply walk down the hall to verify who it is.

A multidisciplinary team made up of professionals from areas such as internal audit, risk management, IT, cybersecurity, and other relevant functions can monitor advances in AI and continuously provide updates to risk management, security protocols, and fraud detection systems. The team can work together to identify and respond to efforts, considering issues such as which controls will best prevent or limit damage, Niedzielski says.

He also recommends companies regularly share their experiences and discuss the AI vulnerabilities that others have faced. "Not only successful efforts, but also times when something has gone wrong and how the company learned from it," he advises. "Knowledge sharing, training, and proper risk assessments will make it possible to minimize the risk of AI-induced fraud."

In this environment, training should be a top priority to increase employee awareness about potential suspicious activities while reinforcing appropriate courses of action to remedy breaches, Niedzielski says. Cacciapuoti notes that it's also possible to use AI simulations to provide cybersecurity training in real time in real-world situations. AI can analyze individual employee behavior in cyber training and provide insights for improvement.

Internal Audit's Contribution

Internal audit can help ensure the organization's efforts match the challenges of AI, Cacciapuoti says, including harnessing the potential while mitigating the risk. "Internal audit should conduct a comprehensive risk assessment, auditing AI systems for security, ethics, and compliance and supporting safe innovation," he says. "It can participate in shaping a cyber strategy that is robust enough to cope with AI threats."

In addition, while internal audit is typically a key line of defense, Cacciapuoti says it should also serve as an offensive line where AI is concerned, taking a dynamic approach in managing risk. "Why wait for risk to arrive when you can attack it head on?" he

> "AI will never replace internal auditors, but it can be a powerful assistant."
>
> **— Antonio Cacciapuoti, CIA**

asks. That means being in the forefront of using new technologies so that the organization can maximize opportunities while ensuring appropriate governance controls and continuous improvement.

Within the internal audit function, "AI will never replace internal auditors, but it can be a powerful assistant," according to Cacciapuoti. He says that internal audit can benefit from using AI to:

- Analyze large volumes of data and expand samples in testing to be very close to the entire population size.
- Automate testing procedures and monitor key controls, taking on repetitive tasks so that internal audit professionals can focus on higher-level tasks.
- Use AI algorithms to monitor data continuously rather than relying on periodic audits, pinpointing and addressing unusual activities that much sooner.
- Use predictive analytics to project future results and make more informed decisions and recommendations.
- Quickly summarize workpapers so that internal auditors can use them in crafting final reports.

AI allows for more uniform and efficient management of findings across all control functions. "In a very large company, there are many engagements from multiple functions to consider," Cacciapuoti says. AI enables internal auditors to pull the data together in a uniform way to avoid duplication.

To mitigate the risks and take advantage of the value, Niedzielski recommends that internal auditors continuously update their knowledge on technology advancements. "There's something new every day," he says. They should focus on identifying proactive — as opposed to reactive —responses to potential risks. As the world attempts to harness new technologies, internal auditors should also focus on governance and compliance with new regulations and ethical standards to safeguard organizational integrity, he says.

AI-powered Cyber Threats: Fast Facts

- 97% of security professionals are concerned their organization will experience an AI-generated cybersecurity incident, as AI continues to cause burnout.
- 75% of security professionals had to change their cybersecurity strategy in the last year due to the rise in AI-powered cyber threats.
- 73% of security teams want to focus more on prevention-first capabilities.
- 61% of organizations saw a rise in deepfake incidents over the past year.
- 75% of these attacks impersonated an organization's CEO or another member of the C-suite.

Source: GenAI in Cybersecurity: Friend or Foe? Voice of SECOPS, Fifth Edition 2024.

"Internal auditors should put themselves in the shoes of a bad actor," according to Niedzielski. "Don't ask how a bad actor would infiltrate the organization, ask what you would do if you were a bad actor based on what you know about the organization. Take into account not only a quantitative, but also a qualitative, perspective on the organization."

Internal auditors should not try to go it alone, says Cacciapuoti, who recommends coordination with all assurance providers and stakeholders to prevent and mitigate risk, including those in the control functions, compliance, risk management, external auditors, and regulators. "Collaboration between AI tools and cybersecurity professionals, alongside a strong governance framework, is essential to navigate this landscape and respond to new and emerging risks," he says.

PART 2

Ensuring Cyber Resiliency

About the Experts

DC Chang, CPA, CDPSE, CISSP, CRISC, CISA

DC Chang is audit director, Digital Technology and Cybersecurity, at United Airlines in Dallas, Texas.

Michael Echols, CISSP

Michael Echols is CEO of Max Cybersecurity LLC in Washington, DC.

Justin Headley, CPA, CISSP, CISA, CRISC

Justin Headley is senior manager in Warren Averett's Risk Advisory & Assurance Services Group in Birmingham, Alabama.

Even as organizations work to ensure they have adequate tools to prevent cyberattacks, it is almost guaranteed they will experience breaches or incursions of some form. With that in mind, businesses also must focus on their ability to respond to and recover quickly from a cyberattack. This brief discusses how best to understand and instill resilience to attacks and describes the internal auditor's role in strengthening an organization's response.

Setting the Stage for Recovery

At its best, cyber resilience is not just a reaction to a dire situation. It is a continuum of practices — planning, processes, analysis, training, critical services, and management — that ensure an organization can maintain operations, according to Michael Echols, CEO of Max Cybersecurity LLC. These practices make it possible to restore or maintain organizational functions after an attack, but they must be set in place long before a problem occurs.

For example, Echols worked with a law firm client that received all its referrals through its website. It typically received many referrals daily, but at one point, two to three days passed before the firm noticed it was not receiving any and ultimately realized it had been hacked. "The firm should have already had a process for continuous monitoring and for some type of notification" about an unusual drop in web referrals, as they were the firm's main source of business (a critical function), he says.

The problems to be identified — like a drop in web traffic — will be different for every business and there likely will be more than one. In many cases, organizations will want to be prepared for an incident that will affect their power supply, for example, with steps to deploy generators that are independent of the main business, so they are not affected by the attack, Echols says.

> Cyber resiliency is "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment."
>
> **— U.S. National Institute of Standards and Technology**

Preparing for what comes next requires putting the current cybersecurity environment in context, according to DC Chang, audit director, Digital Technology and Cybersecurity, at United Airlines. Twenty years ago, organizations had their own data centers, and cybersecurity was, to some extent, a matter of locking up the servers behind physical doors and windows. Today, data is stored in a virtual environment that can be vulnerable to bad actors around the world.

"There are thousands and thousands of windows and doors we need to keep track of now that we're digital, and they're being added and removed on a daily basis," Chang says. Organizations need to be aware of the pace and scope of digital acceleration to develop the resilience they will need in a crisis.

Governance and Culture

Governance has a key role in building cyber resilience, according to Justin Headley, senior manager in Warren Averett's Risk Advisory & Assurance Services Group. "We continually hear that employees are the weak point because they use a weak password or click on suspicious links," he says. "But if leaders are not bought in, you can't expect employees to do their part."

In many ways, cybersecurity is not entirely a technology issue, it is a culture concern. “If you change the minds of 90% of the people in the organization and one person opens a link in an email, it could sink the company,” Echols says. A cybersecurity-aware culture clarifies the organization’s expectations and reassures consumers and business partners. “Banks were one of the first groups to become cyber resilient,” he says, because they rely on the confidence of their stakeholders.

Headley recommends leaders foster a cybersecurity culture that goes beyond standard approaches such as quarterly emails containing cyber safety tips or rudimentary annual security training. Steps his organization takes include sending out its own fake phishing emails to employees, then providing training to those who click on the embedded suspicious links. “You have to show how cyber governance works in action, not just in theory,” he says.

Leaders also can provide specific steps to take in an attack. “An organization can stop an attack and recover if there are practical, repeatable policies and procedures to follow in a breach,” according to Headley. If the leaders are involved when these steps are tested and take part in working out the kinks, they demonstrate their commitment to the effort, which can play a large role in making their cybersecurity strategy successful.

- 68% of breaches involved a non-malicious human element, such as someone falling for a social engineering attack or making an error.
- The median time for users to be taken in by phishing emails was less than 60 seconds.
- 15% of breaches involved a third party or supplier, including software supply chains, hosting partner infrastructures, or data custodians.

Source: Verizon Business 2024 Data Breach Investigations Report

The Impact of Regulation

Under the finalized rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, the U.S. Securities and Exchange Commission raised expectations for organizations by requiring public companies to disclose material cybersecurity incidents and make periodic disclosures on how they assess, identify, and manage cyber risks. The rule “highlights a major table stakes issue that every entity on the planet has to consider,” Chang says.

Among other requirements, the rule forces organizations to ensure their cyber practices are operational, Headley says. He notes that the IT function often operates within a silo, with implied trust from leaders who may not fully understand its workings. “That will have to change,” he says. There will have to be an organizationwide understanding of how to treat internal and customer data and address cyber concerns.

As is the case with many regulations, “it will all come down to transparency,” Echols says. “When there has been a material breach, the company must have a clear process for how it reacts to that breach.”

Adding AI to the Mix

Artificial intelligence (AI) can be an invaluable tool in enhancing prevention of cyber issues and resilience in the wake of an attack. Technology such as next-generation firewalls and point protection systems are making it easier to sort through the data traffic and find anomalies that should be investigated, Headley says. “The use of AI has been a game changer in the last several years, and it will continue to help companies get better at detecting and responding to attacks.”

AI also can be used as a weapon against organizations. “If you have vulnerabilities that have been ignored, AI will help hackers find them,” Echols says.

Among other considerations, organizations will have to balance the drive for greater efficiencies to be gained with new tools with the need to protect security and privacy, according to Headley. New technologies help organizations eliminate repeatable tasks, which often involve feeding the programs sensitive information. At the same time, "we continue to see targeted attacks on these technologies because the bad actors know that people do not fully understand the technology," which can make the sensitive data that programs contain especially vulnerable.

In building resilience, organizations will have to train their people in evolving technologies and ensure technology use matches the organization's risk appetite. "A company could have the best technologies and skills, but a user may still unknowingly or sometimes knowingly leak data through the front door using a GenAI tool," Headley says.

Organizations should also be careful not to neglect traditional cyberattack approaches. Many cyber issues are caused by problems that are not new, such as misconfigurations or failure to follow an established practice, Echols says. Many breaches relate to known vulnerabilities that have never been fixed or patches that have not been installed, he says. As a result, educating end users about new and existing threats is particularly important. "Auditors must look under the hood and ask the right questions of clients to unearth hidden vulnerabilities created by apathy," he says.

> "Stakeholders, primarily an organization's board and senior management, rely on independent, objective, and competent assurance services to verify whether cyber incident response and recovery controls are well designed and effectively and efficiently implemented. The internal audit function adds value to the organization when it provides such services in conformance with the Standards and with references to widely accepted control frameworks, particularly those expressly used by the organization's information technology and information security functions."
>
> **Source: Global Technology Audit Guide: Auditing Cyber Incident Response and Recovery, 2nd Edition, Global Practice Guide, The Institute of Internal Auditors, 2024**

How Internal Audit Can Help Enhance Resilience

In this environment, internal audit should be prepared to frame the outcomes of their audits to enhance resiliency and identify vulnerabilities in ways that help clients understand the potential consequences of lax cybersecurity, Echols says. While clients may assume the worst could never happen to them, internal auditors must be able to suspend disbelief, which will better enable them to imagine the unimaginable. For example, Echols had a client that had a best practice that prohibited use of corporate email addresses in social media accounts, but it was not an official policy. The error of that approach became clear when MGM suffered a significant data breach late last year. Investigation of the breach reportedly revealed that an employee was using their work email on a social media platform. The hackers found the employee's information on LinkedIn and impersonated the employee in a call to MGM's IT help desk, thereby obtaining credentials to access and infect MGM's systems. "Best practices are derived from the experiences of many and should be made policy, when possible," Echols says.

Internal auditors must also understand that the compliance aspect of the audit is only the first step in helping build cyber resilience. "Compliance is not security," Echols says. Internal auditors should focus on translating their findings into greater insights that the client team can use to enhance security and on asking questions the team may not yet be able to answer.

“You should be able to instruct the client that not seeking and finding the answer to this question actually creates a vulnerability,” according to Echols.

Between audits, internal audit should keep the lines of communication open by scheduling times to check in and learn about teams’ challenges. “When internal auditors are able to position themselves as trusted advisors, it’s a complete game changer,” Headley says.

Transparency is crucial. Internal auditors should be clear on the scope and the planned testing procedures, as well as what issues have arisen. “Make sure to communicate early and often,” he says, “especially when it involves IT risk.” He advises that internal auditors avoid rushing to judgment immediately, but instead have an open conversation about the client team’s thought processes and encourage collaboration.

Headley notes that IT teams often get bogged down in meeting the demands of various lines of business, taking responsibility for everything from keeping apps up and running to dealing with day-to-day hardware glitches. As a result, cybersecurity may not always be a top priority. Internal auditors can promote awareness of these challenges and educate teams about opportunities to address them, thereby ensuring audits are a true value-add exercise.

“Internal auditors can be partners in helping to strengthen corporate resilience,” Headley says. Among other steps, they can help smooth out any disconnects between company leaders and IT teams, who often don’t speak the same language. Because internal auditors understand both business risk and IT risk, they can help bridge that gap.

Internal auditors can also shape the understanding of cyber risks and related problem-solving in a way that departs from past practice, Chang says. As organizations move away from traditional business continuity planning or business disaster recovery, internal auditors can help them adopt more multifaceted and nuanced approaches. They can enhance that effort by taking on a role as storytellers who process disconnected information and data points and put them together into a compelling narrative that drives better decision-making.

Evening the Odds

In the end, resilience means accepting the inevitability of attack and assuming that the organization’s outer walls are not impenetrable, Echols notes. As part of that effort, organizations must recognize they are in an unfair fight. While organizations strive to block 100% of the attacks they are facing, hackers only need to open one door to wreak havoc, Chang notes. “It’s a lot more difficult to be the defender than the perpetrator,” he says. Internal audit can provide the insights and information their companies need to improve their odds of cybersecurity success.

According to a survey of IT and security operations decision makers:

- Only 2% of respondents say they could recover their data and restore business processes within 24 hours of a cyberattack.
- 69% say their organization has paid a ransom in the last year, even though 77% say they have a defined policy or protocol against paying ransoms.
- 42% say their organizations could identify sensitive data and comply with applicable data privacy laws and regulations. Others do not have adequate IT and security capabilities to do both.

Source: Cohesity Global Cyber Resilience Report 2024

PART 3

Establishing a New Zero-trust Boundary

About the Experts

Adam Kohnke

Adam Kohnke, based in Madison, Wisconsin, 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, Oklahoma.

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?

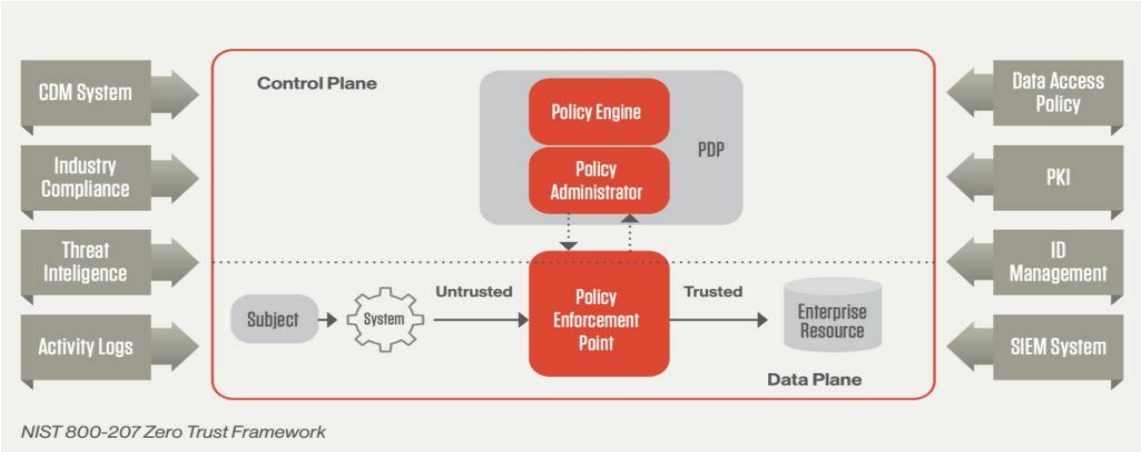
Generally, a zero-trust security framework requires all users that operate within a network — both inside and outside the organization itself — to be authenticated before accessing applications and data, and then continually validated regularly. As the name implies, "trust," or more specifically "trust 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.

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 verify 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.

> 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**

“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.”

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.

Previous Issues

To access previous issues of Global Perspectives and Insights, visit theiia.org/GPI.

Reader Feedback

Send questions or comments to globalperspectives@theiia.org.

About The IIA

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

Disclaimer

Copyright

January 2025

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