

No. 119 | October 2026



Radar

The cybersecurity
magazine

Good governance also means anticipating what comes next

By Diego Javier Rocha Rodríguez

For years, risk management has relied on a familiar approach: identifying, assessing, establishing controls, and conducting periodic reviews. This model remains necessary, but the environment in which organizations operate today is changing at such a pace that the way we govern must evolve as well.

Artificial intelligence is perhaps the clearest example. Its integration into processes, decision-making, data, and systems is creating new opportunities for transformation, but it is also continuously reshaping organizations' risk exposure. Risk no longer changes only when an incident occurs or a new regulation emerges. It can change with a new integration, a new model, a supplier, an automated decision, or a different level of autonomy.

In this context, proactive governance means reducing the gap between the moment risk changes and the moment we are able to identify it and act.

This requires moving from periodic snapshots of risk towards a more dynamic view. It means connecting information from assets, data, identities, suppliers, vulnerabilities, and incidents; detecting early signals; understanding dependencies; and using that context to prioritize decisions before exposure turns into impact.

But having more information and a greater ability to anticipate risk raises another fundamental question: can we trust the intelligence we use to make decisions?

As AI evolves from recommending actions to executing them, trust can no longer be treated as a statement of intent. It must be designed, monitored, and demonstrated. We need to understand how a decision is reached, verify the information that supports it, establish clear boundaries, and maintain mechanisms that allow an action to be challenged, corrected, or reversed when necessary.

In this edition of RADAR, dedicated to Proactive Governance & Risk Management, we explore two sides of the same evolution. In "AI and Corporate Risk: From Periodic Assessment to Continuous Monitoring", we examine how organizations can monitor risk more continuously, correlate signals and anticipate changes in exposure. In "Intelligence We Trust: Trust as the New Frontier of AI", we focus on the conditions required to ensure that this intelligence is understandable, verifiable, controllable and accountable.

Proactive risk management is not about predicting everything that might happen. It is about building the ability to identify change earlier, understand it better and make decisions at the right time. In an environment where technology is constantly evolving, governance can no longer mean simply reviewing what has already happened. It also means being prepared to recognize what is coming next.



Diego Javier Rocha Rodríguez

Cybersecurity Expert Engineer

The Gates of Nanao: Governing Risk Before the Castle Falls

Cyber Chronicle by Juan Pablo Campo Téllez

An organization is not secure simply because it has strong walls. It also needs to know who is able to open the gates. Risk management should not begin when an incident occurs, but much earlier, while there is still time to identify the conditions that could allow it to happen.

In 1576, Uesugi Kenshin, one of the most feared warlords of feudal Japan, led his forces against Nanao Castle in Noto Province. Built on Mount Sekidō and designed to withstand long sieges, Nanao represented exactly what was expected of a fortress of its time: to keep the enemy out.

Kenshin tried and failed. When he returned in 1577, he began a new siege that would last for months. However, the most important battle was no longer taking place in front of its defenses, but within them. An epidemic weakened the defenders, political tensions increased, and internal disputes eventually fractured the structure that held the fortress together.

According to historical records compiled by the city of Nanao, on 15 September 1577, Yusa Tsugumitsu and his allies rebelled and ultimately opened the gates to Uesugi Kenshin's forces. After months of trying to break in, the enemy no longer had to conquer the walls.

Nanao did not fall because its stones were too weak. The fortress fell when the conditions that ensured its security were no longer being governed.

More than four centuries later, organizations continue to build castles. The walls are now firewalls, the watchtowers are security operations centers, the moats are segmentation mechanisms, and the gates are protected by MFA, identity management systems, SIEM, EDR and monitoring platforms.

Companies invest millions in strengthening these defenses, but an organization is not secure simply because it has strong walls. It also needs to know who can open the gates.

That is one of the fundamental principles of proactive risk management. Risk management should not begin when an incident occurs, but much earlier, while there is still time to identify the conditions that could allow it to happen.

An administrative account that retains unnecessary privileges, a supplier with permanent access to a critical environment, a temporary security exception that is never reviewed again, or a legacy system that remains operational may each appear to be justifiable decisions. However, when these decisions accumulate and are no longer properly supervised, they can become the gates of Nanao.

The problem is that risk does not remain static. As the organization evolves, new suppliers, applications, vulnerabilities and identities emerge, while roles, architectures and permissions change. A decision that was acceptable months ago may later become a critical exposure. This is why governing risk requires continuous review of the conditions that can alter it.

One example shows how far this problem can go. In February 2024, Change Healthcare, one of the leading transaction processing platforms in the US healthcare system, suffered a cyberattack that caused major disruptions to services related to prescriptions, medical claims and payments.

The attackers used compromised credentials to gain remote access to a Citrix portal that did not have multifactor authentication enabled. Once inside, they were able to move laterally through the environment, extract information and later deploy ransomware.

The case is particularly relevant because the point of entry was not a sophisticated unknown vulnerability. The access point already existed, was legitimately used for remote access, and simply lacked a safeguard that is now considered essential.

This is precisely where the difference between managing vulnerabilities and governing risk becomes clear. It is not only a matter of asking which vulnerabilities exist, but also which decisions, exceptions and conditions are creating future exposure.

Why does a critical system still operate without MFA? Who accepted that risk? How long was that acceptance meant to remain in place? What mechanism was supposed to verify that the issue had been addressed?

Proactive risk management turns these questions into a continuous process and requires the organization to reassess its decisions as the business changes.

This perspective became even more relevant in February 2024, when NIST published version 2.0 of its Cybersecurity Framework and introduced GOVERN as a sixth function alongside Identify, Protect, Detect, Respond and Recover.

In doing so, NIST made it explicit that cybersecurity management also requires the establishment of risk strategies, responsibilities, policies, oversight mechanisms and processes for managing risk associated with third parties and supply chains. Cybersecurity therefore ceases to be solely the responsibility of those who manage technical tools and becomes part of enterprise risk management and leadership decision making.

A firewall can block a connection, but it cannot decide how much risk an organization is willing to accept. An EDR solution can identify suspicious activity, but it cannot determine who should be accountable for a critical system. An IAM solution can restrict permissions, but it cannot decide why a supplier requires a particular level of access or how long that access should be retained.

These are governance decisions. In other words, someone must know where the gates are, who holds the keys and under what circumstances they may be used.

Proactive risk management means preventing decisions from accumulating unnoticed. It requires clear ownership of risks, expiry dates for exceptions, regular reviews of privileged access, oversight of third parties and mechanisms that can detect when the organization's exposure has changed.

It also requires a culture in which identifying a risk is not seen as a failure. Mature governance does not seek organizations where no one finds problems. It seeks organizations capable of finding them before their adversaries do.

For months, the defenders of Nanao could see the enemy army on the other side of their fortifications. They knew where the threat was and had built defenses capable of keeping it at bay. What they failed to control was the deterioration taking place behind their own walls.

That remains one of the major challenges of modern governance.

A truly resilient organization is not one that assumes its walls are impenetrable, but one that continuously assesses what could weaken them, who can open its gates, and which decisions could turn a fortress into a false sense of security.

Because effective risk management does not begin when the army appears outside the castle. It begins much earlier, while there is still time to decide who holds the keys.



Juan Pablo Campo Téllez
Cybersecurity Engineer

AI and Corporate Risk: From Periodic Assessment to Continuous Monitoring

Article by Ángel Fernando Andrango Mejía

Artificial intelligence is evolving faster than organizations can anticipate its risks. In this context, competitive advantage will no longer depend solely on adopting AI, but on developing the capabilities to identify, understand and govern its risks continuously.

When AI Moves Faster Than Risk Management

Risk matrices remain valuable tools for prioritization and decision making. However, when AI rapidly changes an organization's level of exposure, these tools need to be supported by up to date information on the technologies in use, the data being processed, the access granted, the integrations enabled, the vulnerabilities identified, incidents and operational dependencies.

The objective is not to replace the risk matrix, but to complement it with continuous monitoring capabilities that make it possible to understand how the organization's exposure is changing and support more timely decisions.

In this way, risk management evolves from a periodically reviewed snapshot into a more dynamic view, capable of identifying changes and anticipating scenarios before they result in significant business impact.

The New Generation of Models: What Is Changing?

Market attention often focuses on each new AI model that emerges. However, the real challenge does not lie in any specific technology, but in a deeper trend: the ability of these solutions to continually expand what people and organizations can do.

AI does not only introduce new forms of exposure. It also changes the speed, scale and interdependence of existing risks. A single solution can process sensitive information, connect to critical systems, automate decisions and depend on external providers at the same time.

These capabilities offer significant opportunities for productivity and transformation, but they can also increase exposure just as quickly as the technology is adopted.

Risk arises when these capabilities operate without sufficient visibility, oversight or governance. It is therefore essential to understand where the main exposures may materialize and how they could affect the organization.

Strategic Risks for Proactive Business Management

AI increases the complexity of risk because it brings together data, systems, automated decisions and external dependencies within a single solution.

For this reason, proactive management should consider at least five dimensions:

Data and Privacy

Misuse of sensitive information, new data flows and unexpected access.

Cybersecurity

Impersonation, exploitation of vulnerabilities and integrations with models and agents.

Operations

Technology dependencies, failures, provider changes and the adoption of AI in critical processes.

Compliance and Ethics

Lack of traceability, clearly defined accountability or clear regulatory criteria.

Reputation and Business

Errors or incidents affecting customers, trust, decisions or brand reputation.

AI, therefore, is not a separate category of risk. Its impact spans cybersecurity, privacy, operational continuity, compliance and reputation at the same time.

From a Risk Register to an Intelligent Radar

The main difference between a traditional risk matrix and an intelligent radar lies in the ability to observe how risk evolves.

Risk Matrix

Identify → Assess → Record → Review

Intelligent Radar

Discover → Correlate → Prioritise → Respond → Learn

Both approaches are complementary. While the matrix helps structure and assess known risks, the radar introduces a model of continuous observation that connects signals from different sources to understand how exposure is changing.

This approach makes it possible to:

1. Discover AI tools, models, agents and integrations.
2. Correlate signals from data, users, systems and providers.
3. Prioritize risks with the greatest impact and criticality.
4. Respond through controls and mitigation actions.
5. Learn from incidents and emerging patterns to continuously improve monitoring capabilities.

In short, the matrix shows where the risk is; the radar helps us understand where it is moving.

Indicators that anticipate risk

Continuous observation requires indicators that can identify early warning signs before they develop into incidents or have a significant impact on the business.

Some particularly useful indicators include:

- AI tools without defined governance.
- AI use cases without an assigned business owner.
- AI integrations connected to critical systems.
- Vulnerabilities associated with models, providers or connectors.
- Detection and response times for AI related events.

Continuous measurement of these signals helps identify emerging trends and supports the shift from primarily reactive risk management towards a more preventive and anticipatory approach.

Innovate at Speed, Govern with Foresight

In the coming years, the differentiating factor will not simply be who adopts more artificial intelligence, but who is better able to understand, oversee and govern it.

Organizations that develop continuous monitoring capabilities will be better prepared to capture the benefits of AI while proactively managing its impact on information, security, operations and trust.

Because in an environment where models are constantly evolving, risk can no longer be managed by looking only at the past. It must be managed by watching the horizon.



**Ángel Fernando Andrango
Mejía**
Cybersecurity Lead Analyst

Intelligence We Trust: Trust as the New Frontier of AI

Article by María Pilar Torres Bruna

Artificial intelligence is already capable of surprising us. The next challenge goes deeper: ensuring that its decisions are understandable, verifiable and secure as it gains greater autonomy.

Today, artificial intelligence can already write, analyze, predict, recommend, automate processes and support decisions that once depended entirely on people. Its capabilities are extraordinary, but AI has now moved beyond the stage where it needed to prove its potential. We are entering the next phase of adoption, one in which organizations must decide which processes and decisions they are prepared to entrust to it.

As we increasingly rely on AI to answer complex questions and even take action, such as prioritizing an alert, approving a transaction, interacting with a customer or recommending a critical decision, trust becomes an essential condition for expanding its use and adopting it with confidence. AI is already helping us build more capable and more impressive systems. The focus now is on making them trustworthy.

This changes both the conversation and the architecture that supports AI within an organization. Trust is much more than a statement of principles or a security policy. It must become an operational capability that organizations can design, implement, monitor and demonstrate.

From Fascination to Trust

In recent years, we have explored what AI can create, how much it can help organizations accelerate their business and which tasks it can transform.

However, as the technology begins to operate with greater autonomy, we need to understand how it reached a conclusion, what information it used, what its limits are and who can intervene if something does not work as intended. We need transparency and traceability in the processes behind this technology.

AI can create intelligence, and agents can turn that intelligence into action. Trust is what makes that action acceptable, secure and scalable.

An organization can incorporate AI into many different processes, but it must be able to explain, control and audit the decisions it makes. Without this capability, scaling the use of AI will be difficult, as will building trust among employees and customers. Trust is what makes it possible to move from an appealing proof of concept to real adoption.

Three Questions for Building Trust

A simple way to approach this challenge is to start with three fundamental questions.

1. Can We Understand It?

If a system recommends an action, the people responsible must be able to understand, at least to a level appropriate to the context, why it did so.

Transparency and traceability make it possible to explain how the information provided led to a particular outcome, understand the recommendation and explain it when necessary.

This is especially important in high impact decisions that affect people's lives, such as their professional careers, or that may even help save a life. If an AI system suggests blocking a transaction, rejecting a candidate, prioritizing a medical case or allocating a resource, the decision must be explainable.

2. Can We Verify It?

The quality of an AI response depends on the quality of the information it receives. Data must be complete and up to date, and organizations must ensure that it has not been manipulated.

Trust begins at the source of the data. Organizations need to know where the information comes from, who modifies it, when it was modified and whether any other changes have been made.

The change process must be traceable, as traceability is becoming increasingly important in an environment where synthetic content, data from multiple sources and automated decisions are constantly circulating.

Verification also means validating the authenticity of the content and the identities involved. The source, whether an organization, a person or even an agent, must be trustworthy.

In the age of AI, understanding the origin and integrity of information is no longer simply a technical requirement. It becomes a condition for trust.

3. Can We Challenge It?

The final element of trust is having mechanisms in place to oversee, challenge, correct or reverse decisions made by AI when the context requires it.

Trustworthy AI, and AI based agents, must have clear boundaries. They need to know what they are allowed to do, what information they can access and when they must escalate a decision to a person. It must also be possible to intervene when we detect unexpected behaviour, a deviation from established rules or signs of manipulation.

This is where collaboration between AI and cybersecurity takes on a new dimension.

The Zero Trust approach, traditionally applied to users, devices and connections, is also relevant and useful for intelligent systems. The principle is simple: trust nothing by default. Every agent, model or component should operate with clearly defined permissions, minimum necessary access and continuous validation.

Active Security for Evolving Systems

The risks associated with AI go beyond infrastructure and data. The models used to support decision making represent a new attack surface. An attacker may try to manipulate information sources, alter an agent's permissions or influence the behaviour of a model. For this reason, security must evolve from reactive to active and predictive.

Active cyber defense and predictive security can help detect patterns, correlate large volumes of alerts and respond to certain threats more quickly.

Mature autonomy is supervised autonomy: capable of acting, but also accountable for its actions.

Governing AI Means Governing Its Decisions

When an intelligent system participates in relevant processes, governance cannot be added at the end. It must be built in from the design stage.

This means defining clear owners, decision rights, escalation processes and criteria for intervention. It also requires generating evidence through records that make it possible to review what happened, which data was used, which rules were applied and why the system took a particular action.

Explainable audit trails are essential for turning AI into a supervised capability. They help us respond when something goes wrong and make it possible to learn, improve controls and strengthen trust among customers, employees, regulators and partners.

Trust is not what an organization says about its AI. It is what it can prove, monitor and govern.

The Human Dimension of Trust

Finally, there is one dimension that no technology can address on its own: the human dimension.

People do not assess trust based solely on accuracy metrics. We also consider whether a system is fair, whether it respects privacy, whether it responds within a reasonable timeframe and whether there is still room for human judgement, especially in sensitive decisions.

What people consider acceptable in one context may not be acceptable in another. Expectations vary according to culture, industry, the type of decision involved and the impact that decision has on people.

Building trust in AI requires listening. This means understanding how users perceive risk, what level of autonomy they are willing to accept and under what conditions they consider it legitimate for a machine to participate in a decision that affects them.

Making Trust Operational

Turning trust into an operational capability means advancing on three fronts at the same time:

Make AI understandable: explain decisions and verify content, sources and data provenance.

Make AI controllable: establish boundaries, manage permissions, supervise agents and detect manipulation or deviations.

Make AI accountable: create evidence, traceability and audit mechanisms that make it possible to intervene and correct.

Artificial intelligence will continue to advance. It will become more powerful, more integrated and more autonomous. But its true value will depend on the trust it is able to generate.

Because in the next stage of AI, we will stop asking “Can it do it?” and start asking “Can we trust what it does?”



María Pilar Torres Bruna
Head of Cybersecurity IBIOL

Vulnerabilities

Critical Vulnerability in Cisco Nexus 9000 – Remote Code Execution

Date: September 2, 2026

CVE: CVE-2026-20212



CVSS: 9.8

CRITICAL

Description

Cisco has disclosed a vulnerability affecting certain Nexus 9000 Series switches equipped with Silicon One technology, with a CVSS v3.1 score of 9.8.

An unauthenticated remote attacker could exploit this vulnerability to execute code with root privileges on the affected devices. The issue lies in the exposure of TCP ports 43210 and 43211 within the Layer 3 VRF used by default.

This type of network equipment is commonly deployed in critical data center infrastructure, where a compromise could have a significant impact. For this reason, affected devices should be reviewed as a priority.

Solution

Cisco recommends the following actions:

- Use infrastructure access control lists, or iACLs, to allow only the necessary traffic to the affected device.
- Apply the patch for Cisco NX-OS Software:
 - Live Protect Shield Software - 10.6(3)

Affected Products

The following Cisco Nexus 9000 identifiers are affected:

- N9324C-SE1U y N9348Y2C6D-SE1U
- N9364E-SG2-O/Q
- N9396T12C-SE1 and N9348Y12C-SE1
- N9336C-SE1
- N9K-C9804 and N9K-C9808

References

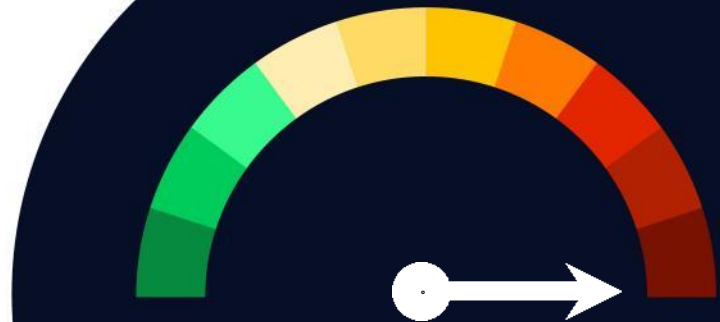
- nvd.nist.gov
- rapid7.com

Vulnerabilities

Critical Vulnerabilities in SonicWall SMA1000 Under Active Exploitation

Date: September 1, 2026

CVE: CVE-2026-83548 and 1 more



CVSS: 10

CRITICAL

Description

SonicWall has disclosed two vulnerabilities affecting SonicWall SMA1000 devices:

- **CVE-2026-83548:** A pre-authentication SSRF vulnerability that allows an unauthenticated remote attacker to send requests to internal resources.
- **CVE-2026-83549:** A post-authentication OS command injection vulnerability that allows an attacker with administrative privileges to execute arbitrary commands on the appliance's operating system.

Both vulnerabilities have been actively exploited, as confirmed by SonicWall's incident response team.

Solution

The vendor recommends that all organizations using affected devices take the following actions:

- Update to the latest version available on the official website.
- Review systems for indicators of compromise with the support of SonicWall technical assistance.
- If IOCs are identified on any system, the recommended actions are:
 - Reinstall the operating system or virtual appliances.
 - Reset all user and administrator passwords.
 - Reset TOTP tokens.

Affected Products

The products affected by these two vulnerabilities are SonicWall SMA 1000 series models **6210, 7210 and 8200v** in the following versions:

- **12.4.3-03453** and earlier.
- **12.5.0-02835** and earlier.

References

- sonicwall.com
- rapid7.com
- securityweek.com

Patches

Microsoft Security Patch for Critical Vulnerabilities in SQL Server 2022

Date: September 8, 2026

CVE: CVE-2026-67378

High

Description

Microsoft has released several new security updates aimed at fixing vulnerabilities affecting both Windows and Linux installations. Within the GDR branch.

These patches fix different vulnerabilities such as remote code execution, privilege escalation, information disclosure, denial of service, and security feature evasion mechanisms.

Among them, the most prominent vulnerabilities are CVE-2026-67378, a remote execution vulnerability with CVSS 8.5, in addition to CVE-2026-67380, CVE-2026-67384, and CVE-2026-67385, which reach CVSS 8.8.

Affected Products

The affected products are:

- SQL Server 2022 RTM GDR.

Solution

Install the following security patches:

- KB5122771
- KB5122768

References

- support.microsoft.com
- catalog.update.microsoft.com

Patches

Adobe Commerce Security Patch

Date: September 7th, 2026

CVE: CVE-2026-75650

Critical

Description

Adobe has released an urgent security patch to fix a critical vulnerability (CVSS 10.0) affecting Adobe Commerce/Magento that is being actively exploited in real-world attacks.

The CVE-2026-75650 vulnerability, also known as StyleSmuggler, affects the Adobe Commerce/Magento templating system, allowing a remote and unauthenticated attacker to send a specially manipulated request to get PHP code execution on the server.

In recent real attacks, this flaw has been observed to be exploited to deploy a backdoor developed in Rust, as well as to install a PHP web shell within the Magento image directory.

Affected Products

The products affected by this critical vulnerability are:

- Adobe Commerce versions 2.4.4-2026-aug through 2.4.9-2026-aug, and earlier versions within those branches.
- Adobe Commerce B2B versions 1.3.3-2026-aug, 1.3.4-2026-aug, 1.4.2-2026-aug, 1.5.2-2026-aug and 1.5.3-2026-aug, and earlier.
- Magento Open Source versions 2.4.6-2026-aug through 2.4.9-2026-aug, and earlier.

Solution

The vendor recommends immediately applying patch **VULN-39341** and rotating encryption keys and any potentially exposed credentials, including administrator, server, database, API and integration credentials.

Additionally, it is recommended to review the **IOCs** identified in the observed attacks.

References

- helpx.adobe.com
- experienceleague.adobe.com
- sansec.io
- thehackernews.com

Events

ISACA 2026 Europe Conference

October 7 - 9

The ISACA Europe Conference will bring together professionals and leaders in technology, cybersecurity, audit, governance and risk management in Munich and online. With its focus on governance, risk and decision-making, the event is especially relevant for organizations looking to stay ahead in an increasingly dynamic technology landscape.

[Link](#)

ISC2 Security Congress 2026

October 24 - 28

Cyber Security & Cloud Expo Europe will bring together cybersecurity, technology and digital transformation leaders in Amsterdam. The agenda will cover cybersecurity leadership, enterprise risk, cloud security, artificial intelligence, identity, Zero Trust and compliance.

[Link](#)

Cyber Security & Cloud Expo Europe 2026

October 19 - 20

ISC2 Security Congress will bring together professionals from the global cybersecurity community in Denver and online. The 2026 edition includes sessions on leadership, risk management, AI security and oversight challenges in the face of innovation.

[Link](#)

Resources

➤ **The new rules of trust: Governance, risk and compliance in the AI era**

NTT DATA publication analyzing how artificial intelligence, cloud technologies, digital ecosystems and regulatory developments are transforming traditional governance, risk and compliance models. It explores the shift towards a more integrated and proactive approach to GRC.

[Link](#)

➤ **NIST CSF 2.0: Cybersecurity, Enterprise Risk Management and Workforce Management Quick-Start Guide**

World Economic Forum report, produced in collaboration with Accenture, analyzing the main factors reshaping the global cybersecurity landscape: artificial intelligence, geopolitical fragmentation, supply chains and capability gaps.

[Link](#)

➤ **Global Cybersecurity Outlook 2026**

NIST guide published in March 2026 that connects cyber risk management with enterprise risk and the capabilities needed to respond to an evolving technology environment.

[Link](#)



Subscribe to RADAR

up.nttdata.com/suscribetearadar

**Powered by the
cybersecurity
NTT DATA team**

es.nttdata.com